Proveedor de Certificados PROCERT, C.A.
Declaración de Prácticas de Certificación (DPC)
Para la infraestructura de clave pública de recursos (RPKI)

Fecha	Octubre 2025
Edición	25
Versión	1
Elaborado por	Gerencia General octubre 2025
Aprobado	Alta Dirección octubre 2025
Descripción	Declaración de Practicas de Certificación (DPC)
Vigente	Si

Página

1. Introducción.

Este documento es la Declaración de Prácticas de Certificación (CPS, por sus siglas en inglés) de Proveedor de Certificados PROCERT, C.A. Describe las prácticas empleadas por la entidad de certificación (CA) Proveedor de Certificados PROCERT, C.A en la infraestructura de clave pública de recursos (RPKI). Estas prácticas se definen de acuerdo con los requisitos de la Política de Certificados (CP) [RFC6484] para el RPKI.

El RPKI está diseñado para admitir la validación de las notificaciones por parte de los titulares actuales de recursos numéricos de Internet (INR) (Sección 1.6) de acuerdo con los registros de las organizaciones que actúan como CA en esta RPKI. La capacidad de verificar tales afirmaciones es esencial para garantizar la distribución única e inequívoca de estos recursos.

Esta PKI es paralela a la jerarquía de distribución INR existente. Estos recursos son distribuidos por la Autoridad de Números Asignados de Internet (IANA, por sus siglas en inglés) a los Registros Regionales de Internet (RIR, por sus siglas en inglés). En algunas regiones, los Registros Nacionales de Internet (NIRs) forman un nivel de la jerarquía por debajo de los RIRs para la distribución de INR. Los proveedores de servicios de Internet (ISP) y los suscriptores de red forman niveles adicionales debajo de los registros.

Convenciones utilizadas en este documento:

Las palabras clave "DEBE", "NO DEBE", "REQUERIDO", "DEBERÁ", "NO DEBERÁ", "DEBERÍA", "NO DEBERÍA", "RECOMENDADO", "PUEDE" y "OPCIONAL" en este documento deben interpretarse como se describe en [RFC2119].

Igualmente, el presente documento se constituye en la declaración por parte de Proveedor de Certificados PROCERT, C.A., a los fines de informar y documentar sus procesos de certificación, para una mejor comprensión y entendimiento por parte de su la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada.

La presente Declaración de Prácticas de Certificación permite a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada de Proveedor de Certificados PROCERT, C.A., conocer cada uno de los procesos y subprocesos involucrados en ciclo de vida de los certificados electrónicos; documentar los procesos de recuperación ante desastres, manejo de claves criptográficas y dar una visión general de los equipos e infraestructura que soporta el esquema de confianza en la RPKI de Proveedor de Certificados PROCERT, C.A.

1.1. Descripción general.

La Declaración de Prácticas de Certificación (DPC) se constituyen en la guía de mejores principios de gestión y operación de Proveedor de Certificados PROCERT, C.A., los cuales se encuentran ajustados a los requisitos básicos para la emisión y administración de certificados S/MIME de confianza pública del CA / Browser Fórum y es parte de la documentación que debe mantener Proveedor de Certificados PROCERT, C.A. para la operación de su RPKI. El presente documento de la Declaración de Prácticas de Certificación (DPC) de Proveedor de Certificados PROCERT, C.A. se ajusta de forma periódica y aplica a la Autoridad de Registro (AR) de Proveedor de Certificados PROCERT, C.A.,

debiendo ser informado todo cambio a la Alta Dirección, personal, Clientes, Proveedores y Parte Interesada del PSC PROCERT.

La presente Declaración de Prácticas de Certificación (DPC) de Proveedor de Certificados PROCERT, C.A., contempla los certificados emitidos por la RPKI de Proveedor de Certificados PROCERT, C.A., bajo la Raíz de Certificación del Estado Venezolano (RCEV) y a través de una SubCA que está firmada por la CA Raíz del Estado Venezolano, la cual es administrada y controlada por la Superintendencia de Servicios de Certificación (SUSCERTE) ente perteneciente al estado venezolano. La SubCA de Proveedor de Certificados PROCERT, C.A., cumple el estándar y normas internacionales aplicables a una RPKI conforme a lo establecido en el del CA / Browser Fórum, respecto al Grupo de trabajo de certificados de servidor, la emisión y administración de certificados S/MIME de confianza pública, el grupo de trabajo de seguridad de red y grupo de trabajo de certificado de firma de código; la emisión de certificados adicionalmente cumple toda la normativa emanada de la SUSCERTE y la legislación vigente de la República Bolivariana de Venezuela en materia de certificados electrónicos y la operación de Proveedores de Servicio de Certificación (PSC). Respecto a los Signatarios, cumplimos con los términos y condiciones establecidos en el contrato de uso del servicio de suministro de certificado de firma electrónica para entidad final.

1.2. Nombre e identificación del documento.
El nombre de este documento es Proveedor de Certificados PROCERT, C.A., Declaración de Prácticas de Certificación para la infraestructura de clave pública de recursos (RPKI)". https://www.procert.net.ve/Internas/AC.aspx. Esta Declaración de Prácticas de Certificación (DPC) ha sido objeto de cambios y ajustes, los cuales se listan a continuación indicando las ediciones y versiones que se encuentra modificadas y la edición vigente con su versión correspondiente:

Versión	Motivo de Cambio	Publicación	Vigencia
Edición 01	Emisión	01/01/2008	No
Edición 02	Corrección Semestral (Actualización)	08/07/2009	No
Edición 03	Control y Corrección Semestral (Actualización)	05/01/2010	No
Edición 04	Control y Corrección Semestral (Actualización)	29/07/2010	No
Edición 05	Control y Corrección Semestral (Actualización)	13/01/2011	No
Edición 06	Control y Corrección Semestral (Actualización)	16/06/2011	No
Edición 07	Control y Corrección Semestral (Actualización)	03/01/2012	No
Edición 08	Control y Corrección Semestral (Actualización)	16/07/2012	No
Edición 09	Control y Corrección Semestral (Actualización)	26/02/2013	No
Edición 10	Control y Corrección Semestral	22/08/2013	No

	(Actualización)		
Edición 11	Control y Corrección Semestral (Actualización)	15/01/2014	No
Edición 12	Control y Corrección Semestral (Actualización)	10/07/2014	No
Edición 13	Control y Corrección Semestral (Actualización)	17/11/2014	No
Edición 14	Control y Corrección Semestral (Actualización)	07/04/2015	No
Edición 15	Control y Corrección Semestral (Actualización)	06/10/2015	No
Edición 16	Control y Corrección Semestral (Actualización)	01/02/2016	No
Edición 17	Control y Corrección Semestral (Actualización)	16/03/2016	No
Edición 18	Control y Corrección Semestral (Actualización)	09/05/2016	No
Edición 19	Control y Corrección Semestral (Actualización)	05/06/2017	No
Edición 20	Control y Corrección Semestral (Actualización)	11/07/2017	No
Edición 21	Control y Corrección (Actualización Técnica)	22/09/2017	No
Edición 22	Control y Corrección (Actualización Técnica) Control, Revisión y Ajuste por Remediación de Acreditación 2019.	06/01/2018 06/06/2018 05/01/2019 07/07/2019 06/11/2019	No
Edición 23	Control, Revisión y Ajuste Semestral (Actualización) Control y Ajuste (Actualización) Migración Daycohost. Control, Revisión y Ajuste Semestral (Actualización) Control, Revisión y Ajuste Semestral (Observación de informe de Auditoría SUSCERTE 2023 apartado C1) Control, Revisión y Ajuste Semestral (Actualización) Cambio de Algoritmo	02/08/2020 07/06/2021 07/12/2021 08/06/2022 06/12/2022 10/01/2023 17/07/2023 14/12/2023 24/02/2024 10/06/2024 10/10/2024	No

Edición 24	Estandarización al CA /Browser Fórum	17/08/2025	No
Edición 25	Estandarización al CA /Browser Fórum	28/10/2025	Si

1.3. Participantes de RPKI.

A continuación, se procederá a informar acerca de las entidades que forman parte de la RPKI bajo el esquema de certificación aplicable y aceptado dentro de la República Bolivariana de Venezuela.

1.3.1. Autoridades de certificación.

La Autoridad de Certificación del Estado Venezolano se crea por Decreto Ley Presidencial, donde igualmente se crea a la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), que es la entidad de gobierno encargada de administrar la Autoridad de Certificación (AC) Raíz del Estado Venezolano, que es la encargada, previo cumplimiento de normas y requisitos, de emitir los certificados de las SubCAs que operan dentro de la República Bolivariana de Venezuela y conforme a sus leyes, como Proveedores de Servicios de Certificación (PSC) y que son las encargadas de emitir certificados electrónicos para usuarios o entidades finales.

La AC Raíz del Estado Venezolano cumple con publicar de forma periódica su Lista de certificados Revocados (LCR); e igualmente mantiene a disposición un servicio en línea OCSP para la validación de los certificados de las SubCA que se encuentren bajo dicha raíz de certificación. La dirección de validación y acceso a la LCR de Proveedor de Certificados PROCERT, C.A., es la siguiente https://www.procert.net.ve/Internas/AC.aspx. La dirección de acceso al servicio OCSP de Proveedor de Certificados PROCERT, C.A., es la siguiente. http://ocsp.suscerte.gob.ve.

Proveedor de Certificados PROCERT, C.A., es una empresa privada no perteneciente a ninguna entidad de gobierno, que opera su propia RPKI bajo esquema de SubCA subordinada a la AC Raíz del Estado Venezolano y que se encuentra debidamente acreditada y autorizada por la SUSCERTE para emitir certificados electrónicos para usuarios finales.

La SubCA de Proveedor de Certificados PROCERT, C.A., es una AC que presta servicios al público en general prestado sus servicios como PSC y emitiendo certificados para entidades finales, cumpliendo y manteniendo actualizados, todos los requisitos establecidos por el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela, aplicables para operación de una RPKI. La dirección de validación y acceso a las LCR de la SubCA de Proveedor de Certificados PROCERT, C.A., es la siguiente: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl. La dirección de acceso al servicio OCSP de las SubCA de Proveedor de Certificados PROCERT, C.A., para S/MIME es la siguiente: http://ocspsmime.procert.net.ve/ocsp. Proveedor de Certificados PROCERT, C.A., no posee RPKI tercerizadas o gestionadas por terceros.

Para el momento de emisión de la presente DPC la RPKI de Proveedor de Certificados PROCERT, C.A. posee una (1) partición identificada de la siguiente manera, SubCA para la emisión y administración de certificados S/MIME de confianza pública. La SubCA para la emisión y administración de certificados S/MIME de confianza pública, se encuentra activa y es designada como una SubCA en producción.

La SubCA para la emisión y administración de certificados S/MIME de confianza pública de Proveedor de Certificados PROCERT, C.A. dentro de sus obligaciones con los Signatarios debe cumplir lo siguiente: i) Gestionar el ciclo de vida de los certificados de los Signatarios; ii) Mantener la LCR y el OCSP activos y dentro del marco autorizado por esta DPC y el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela, aplicables para operación de una RPKI ; iii) Mantener alta disponibilidad en su portal web de gestión de certificados; iv) Mantener actualizada su RPKI y su documentación conforme a los establecido por el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela, aplicables para operación de una RPKI.

Todos los procesos de manejo de contingencia, recuperación ante desastres y manejo de la RPKI se encuentran desarrollados en la presente DPC de Proveedor de Certificados PROCERT, C.A.

1.3.2. Autoridades de registro.

La Autoridad de Registro (AR) es la organización encargada de validar y comprobar la identificación y los datos suministrados por las personas jurídicas o naturales que compren certificados electrónicos y con el fin de poder dar fe pública que el cliente que detenta y usa un certificado electrónico, es quien efectivamente dice ser o representar en el caso de persona jurídica, garantizando de esa manera la identidad del Signatario propietario de un certificado electrónico y en consecuencia, establecer el no repudio, responsabilidad legal y las obligaciones derivadas del uso de la firma electrónica bajo los supuestos del CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

Todos los interesados en obtener un certificado electrónico con valor y prueba legal deben acudir a un PSC acreditado ante la SUSCERTE. Proveedor de Certificados PROCERT, C.A. es un PSC acreditado ante la SUSCERTE que cuenta dentro de su estructura con una AR funcional.

La AR de Proveedor de Certificados PROCERT, C.A. es la encargada de revisar la documentación, correo electrónico, datos de identidad y biometría al igual que los soportes presentados por los Signatarios, a los efectos de realizar la verificación, validación presencial y documental de los registros, soportes y demás documentos que acreditan la identidad y/o representación de los Signatarios, así como su cualidad de representantes de personas jurídicas que opten por un certificado electrónico emitido por el PSC Proveedor de Certificados PROCERT, C.A.

El PSC Proveedor de Certificados PROCERT, C.A. no posee AR tercerizadas o externas. Todos los Signatarios deben atender una entrevista a los fines de ser comprobada su identidad y datos aportados en el proceso de adquisición de un certificado electrónico. Las solicitudes de los Signatarios que no atienda la entrevista pautada por la AR quedarán anuladas y se les aplicará una penalización descartando la consecuencia la solicitud. La documentación soporte utilizada para validar a los Signatarios será almacenada por la AR del PSC Proveedor de Certificados PROCERT, C.A., durante un período de diez (10) años contados a partir de la vigencia del certificado o de cualquiera de sus renovaciones.

La AR del PSC Proveedor de Certificados PROCERT, C.A. opera desde la sede administrativa del mencionado PSC, manteniendo un esquema de gestión orientado a garantizar la continuidad operacional y prestación de servicios con altos estándares de calidad, oportunidad y seguridad. La AR gestiona las solicitudes de los Signatarios respecto al ciclo de vida de los certificados y de los procesos administrativos y legales asociados a la emisión de certificados electrónicos en cumplimiento del CA/Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

Para la fecha de publicación de la presente DPC, la RPKI de Proveedor de Certificados PROCERT, C.A. posee una (1) partición identificada de la siguiente manera, SubCA para la emisión y administración de certificados S/MIME de confianza pública. La SubCA para la emisión y administración de certificados S/MIME de confianza pública se encuentra designada como una SubCA en producción y que la AR se encargará de validar la identificación e información suministrada por los Signatarios que gestionen firmas electrónicas dentro de la República Bolivariana de Venezuela. La información requerida para la emisión de certificados S/MIME de confianza pública, se encuentra detallada dentro del sistema de contratación automatizado en el portal web de Proveedor de Certificados PROCERT, C.A. El uso y atributos del certificado S/MIME de confianza pública se encuentran definidos y establecidos en la Política de Certificados (CP) de Proveedor de Certificados PROCERT, C.A.

Recibida la documentación de los Signatarios que contraten el uso de certificados S/MIME de confianza pública, la AR del PSC Proveedor de Certificados PROCERT, C.A. procederá a fijar oportunidad para que tenga lugar la entrevista de validación de identidad, la cual podré ser presencial, vía web o suplida con un video que suba el Signatario en el portal web de Proveedor de Certificados PROCERT, C.A. Durante la entrevista o producto de la verificación del video subido por el Signatario, el operador de la AR del PSC Proveedor de Certificados PROCERT, C.A. aprobará la solicitud o solicitará la información adicional que sea necesaria a los fines de establecer y garantizar la identidad del Signatario. Aprobada la solicitud se gestionará ante la RPKI de Proveedor de Certificados PROCERT, C.A. la solicitud de emisión de certificado para el Signatario validado. El proceso de gestión se encuentra automatizado y luego de la aprobación del expediente electrónico de cada Signatario, el sistema de la AR informa

a los operadores de la RPKI acerca de las peticiones existente y pendiente de aprobación.

La AR mantiene una lista de distribución para tratar los casos asociados a los tramites de la AR, la dirección es registro_01@procert.net.ve, dicha lista de distribución tiene asociada las direcciones de correo personales del personal de la AR.

1.3.3. Suscriptores.

Son los Signatarios y organizaciones que utilizan los certificados electrónicos de usuario final que son generados por a RPKI de Proveedor de Certificados PROCERT, C.A dentro y fuera de la República Bolivariana de Venezuela. Los Signatarios se encuentran obligados a cumplir las condiciones de la DPC y PC que se establecen respecto al uso autorizado de los certificados electrónicos emitidos por Proveedor de Certificados PROCERT, C.A.

1.3.4. Partes de confianza.

Son todos los Signatarios o entidades que utilizan certificados electrónicos y productos derivados de la RPKI de Proveedor de Certificados PROCERT, C.A. y que, a los fines de establecer el esquema de confianza y validez de los certificados electrónicos, proceden a la validación de la LCR y/o el acceso al servicio OCSP de la RPKI de Proveedor de Certificados PROCERT, C.A, a los fines de comprobar la validez y funcionamiento esperados conforme al estándar internacional y nacional dentro de la República Bolivariana de Venezuela de los certificados electrónicos emitidos por la mencionada RPKI.

Los terceros de buena fe son personas o entidades jurídicas que confían en una firma electrónica, certificado electrónico, lista de certificados revocados o información generada por el PSC Proveedor de Certificados PROCERT y sobre las cuales pueden depositar su confianza de acuerdo con el presente documento de la Declaración de Prácticas de Certificación (DPC). La RPKI del PSC Proveedor de Certificados PROCERT, está contractualmente obligada, directa o indirectamente (mediante cadena de contratos) con todos los clientes, proveedores y/o parte interesada que sean Signatarios o no y que utilicen firmas o certificados electrónicos generados por el PSC Proveedor de Certificados PROCERT.

1.3.5. Otros participantes.

El PSC Proveedor de Certificados PROCERT, C.A. mantiene relaciones comerciales, contractuales y alianzas estratégicas con empresas proveedoras de servicios, software y tecnología que permiten la prestación de los servicios de certificación y de la RPKI.

1.4. Uso de certificados.

Los certificados emitidos por el PSC Proveedor de Certificados PROCERT, C.A. son generados bajo a Raíz de Certificación del Estado Venezolano y permiten establecer la vinculación entre una persona física o entidad con una clave pública, que es producto de una validación de su identidad a través de la AR y es generado por la entidad de confianza Proveedor de Certificados PROCERT,

C.A. a través de su RPKI en cumplimiento de CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

El certificado electrónico generado por el PSC Proveedor de Certificados PROCERT, C.A. funciona como una identificación del Signatario en Internet, permitiendo garantizar la identidad, integridad del dato, el no repudio de la transacción y por ende la prueba legal de la operación o mensaje electrónico, creando un estado de confianza que permite a otros usuarios confiar en el certificado electrónico y en la identidad del Signatario emisor del documento o mensaje electrónico. A través del certificado electrónico generado conforme estándar. que permite de manera segura a otros usuarios confiar en la identidad del usuario en internet, ya que contiene datos como nombre, apellido, número de documento de identidad o colegio profesional, dirección, número de serie del certificado y la clave pública asociada al mismo.

1.4.1. Usos apropiados del certificado.

El uso de los certificados emitidos por la RPKI del PSC Proveedor de Certificados PROCERT, C.A. estará limitados al uso establecido en la CP de la Proveedor de Certificados PROCERT, C.A., firma de certificados electrónicos para autoridades subordinadas, firma de las listas de certificados revocados y la firma de todos los certificados establecidos en la CP en cumplimiento del CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

1.4.2. Usos prohibidos del certificado.

El Signatario y terceras partes de confianza usuarios de certificados electrónicos generados por la RPKI del PSC Proveedor de Certificados PROCERT, C.A. se obligan a utilizarlos conforme a lo descrito en la Sección 1.4.1. y los usos permitidos y señalados en la CP y en el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

1.5. Administración de políticas.

La Alta dirección y personal operativo y de la AR del PSC Proveedor de Certificados PROCERT, C.A. mantendrán la presente Declaración de Prácticas de Certificación (DPC) y la Política de Certificados (PC) actualizadas y conforme a los requerimientos del CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela. En esta sección el Signatario encontrará información de interés respecto a las organizaciones encargadas de la Administración de las políticas y documentos del PSC Proveedor de Certificados PROCERT, C.A.

1.5.1. Organización que administra el documento.

La presente DPC, la PC y documentos relacionados al manejo de la AR y de la RPKI del PSC Proveedor de Certificados PROCERT, C.A. son mantenidos, administrados y actualizados por el oficial de seguridad y cumplimento; todo cambio debe ser aprobado por el Comité de Seguridad de la Información y Riesgo, que se encuentra en la siguiente dirección de contacto: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso

13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela. soporte@procert.net.ve.

1.5.2. Persona de contacto

Consultoría Jurídica que se encuentra en la siguiente dirección de contacto: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela. soporte@procert.net.ve, www.procert.net.ve

Persona contacto para gestionar revocación.

El Signatario a través del sistema AR que se encuentra en el portal web del PSC Proveedor de Certificados PROCERT, C.A. www.procert.net.ve puede revocar su propio certificado de la RPKI. Igualmente, el Signatario podrá informar a la AR acerca de su solicitud fundamentada de revocación del certificado electrónico a través de la dirección registro_01@procert.net.ve. La AR validará la información y se procederá con la revocación. Toda denuncia o reporte respecto a la operación no ajustada de la RPKI debe ser remitida a la siguiente dirección soporte@procert.net.ve, indicando las razones y evidencias. El departamento de operaciones de la RPKI dará respuesta a las denuncias de fallas en la operación de la RPKI.

1.5.2. Persona que determina la idoneidad de CPS para la póliza.

El oficial de seguridad y cumplimento es el encargado de determinar la idoneidad del este documento considerando las opiniones de auditores independientes debidamente acreditados y con credenciales reconocidas por el CA / Browser Fórum y que sean producto de auditorías de seguimiento o acreditación; también se debe garantizar el cumplimento de las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

1.5.4. Procedimientos de aprobación de CPS.

Todo cambio en la presente DPC. en la PC, así como en los manuales operativos del PSC Proveedor de Certificados PROCERT, C.A. y que ameriten una modificación distinta a la revisión semestral de la documentación y derivada de algún cambio en el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela o resultado de remediaciones ordenadas por informes de auditorías de seguimiento o acreditación; debe ser gestionado por el oficial de seguridad y cumplimento por ante el Comité de Seguridad de la Información y Riesgo del PSC Proveedor de Certificados PROCERT, C.A., debiendo ser aprobados los cambios de manera sustentada y con minutas de aprobación del mencionado Comité.

1.6. Definiciones y acrónimos.

Con el objeto de ofrecer una interpretación adecuada al sentido y alcance del presente documento, a continuación, se enunciarán una serie de conceptos, cuyas denominaciones en plural o singular atenderán al significado que se asigna a continuación:

Acuerdo de Parte de Confianza: Significa el contrato de servicio que acepta el Signatario al momento de adquirir un certificado electrónico generado por el PSC Proveedor de Certificados PROCERT, C.A. y que contempla los términos y condiciones aplicables a dicha contratación.

Autoridad de Certificación (AC): Significa una autoridad en la cual confían los clientes y que administra una RPKI destinada a crear, emitir y manejar el ciclo de vida de certificados electrónicos, la cual a los efectos de la legislación venezolana debe contar con la acreditación otorgada por la SUSCERTE y cumplir adicionalmente las normas del CA / Browser Fórum.

Auditoria de Cumplimiento: Significa la revisión y examen del sistema de récords y actividades ejecutada por un profesional autorizado y que tiene como fin evaluar la adecuación y la efectividad de los controles de sistemas para garantizar el cumplimiento con las políticas y procedimientos operacionales establecidos y recomendados para la operación de un PSC y de la RPKI. Detectando los cambios necesarios en los controles, políticas y procedimientos y asegurar la implantación de dichos cambios en el tiempo y en cumplimiento del CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela.

Autoridad de Registro: Significa la entidad cuyo propósito es suministrar apoyo local a la RPKI del PSC Proveedor de Certificados PROCERT, C.A. en el proceso de validación de identidad y documentación de un Signatario que gestiona la compra de un certificado electrónico emitido por el PSC Proveedor de Certificados PROCERT, C.A.

Baseline Requirements (BR) Significa los requisitos básicos de CA/Browser Fórum para la operación conforme de una RPKI y la emisión ajustada de certificados electrónicos para entidades finales. www.cabforum.org.

Cadena de Certificado: Significa una cadena de múltiples certificados necesarios para validar un certificado. Las cadenas de certificado se construyen mediante la vinculación y verificación de la firma electrónica en un certificado con una clave pública que se encuentra en un certificado emitido por el PSC Proveedor de Certificados PROCERT, C.A., la cual se encuentra subordinada y firmada por el certificado raíz del estado venezolano y que es administrado por la SUSCERTE.

Certificado electrónico: Significa una estructura de datos que utiliza el estándar CCITT ITU X.509, que contiene la clave pública de una entidad junto a información asociada y presentada como "un-forgettable" (inolvidable), mediante una firma electrónica de la autoridad de certificación que la generó.

Clave Privada: Significa la clave asimétrica de una entidad, la cual solo será conocida solamente por esa entidad.

Clave Pública: Significa la clave de un par clave asimétrico de una entidad que puede hacerse pública, aunque no necesariamente esté disponible al público en general ya que puede ser restringida a un grupo predeterminado.

Declaración de Práctica de Certificación (DPC): Significa la declaración de las prácticas que utiliza una Autoridad de Certificación en su proceso de generación de

certificados, manejo del ciclo de vida de los mismos, información acerca de los proceso de control de seguridad y mecanismos de remediación de riesgos y procedimientos de recuperación ante desastres, que deben ser del conocimiento de los Signatarios que confían en los certificados electrónicos emitidos por el PSC Proveedor de Certificados PROCERT, C.A.

Infraestructura de clave pública de recursos (RPKI) abierta: Significa toda entidad que posea y administre una AC y que suministre entidades finales, servicios de certificación bajo una PKI que cumpla los estándares y normas impuestos por el CA / Browser Fórum, las normas y procedimientos establecidos por la SUSCERTE y la legislación de la República Bolivariana de Venezuela, para la operación conforme de un PSC.

Integridad de Datos: Significa la cualidad o condición de ser preciso, completo y válido y no ser alterado o destruido de manera no autorizada.

Interoperabilidad: la interoperabilidad implica que los equipos y procedimientos usados por dos o más entidades sean compatibles y, por lo tanto, es posible que asuman actividades en común o relacionadas.

Lista de Certificados Revocados (LCR): Significa la lista de certificados que han sido revocados o suspendidos por el PSC Proveedor de Certificados PROCERT, C.A. y que ya no son de confianza para el público en general. La LCR tiene una vigencia de veinticuatro horas y el publicada por la RPKI de forma periódica cumpliendo el plazo de veinticuatro horas entre cada publicación.

Online Certificate Status Protocol (OCSP) Es un servicio en línea que permite en cualquier momento validar el estado de un certificado electrónico emitido por el PSC Proveedor de Certificados PROCERT, C.A. La respuesta de las solicitudes incluye tres (3) estatus: valido, revocado o desconocido.

Par Clave Asimétrico: Significa el par de claves relacionadas donde la clave privada define la transformación privada y la clave pública define la transformación pública.

Política de certificados CP. Es el documento contentivo del conjunto de reglas y características técnicas y de uso de los certificados electrónicos generados por el PSC Proveedor de Certificados PROCERT, C.A. bajo su RPKI.

PSC: Significa Proveedor de Servicios de Certificación

Registro de Auditoria: Significa la unidad de dato discreta registrada en el rastro de auditoría cuando ocurre un evento que es registrado. Un registro de auditoría consiste en un conjunto de descripciones de auditoría, cada uno de los cuales tiene un conjunto de atributos de auditoría asociados a éste. Cada registro de auditoría tiene una descripción de auditora para el encabezamiento del registro y usualmente tiene descripciones de auditoría adicionales que describen la entidad(es) y objeto(s) involucrados en el evento.

Revocación de Certificado: Significa el proceso que consiste en cambiar el estatus de un certificado de válido a suspendido o revocado. Cuando un certificado tiene estatus revocado, esto significa que una entidad ya no se debe confiar en él para ningún fin.

La revocación en el caso del PSC Proveedor de Certificados PROCERT, C.A. PSC, puede ser autogestionada por e Signatario o solicitada a la AR.

Servicios de Certificación: Significa los servicios que se pueden suministrar con relación al manejo del ciclo de vida de los certificados a cualquier nivel de la jerarquía de la RPKI incluyendo servicios auxiliares tales como servicios OCPS, servicios de tiempo compartido, servicios de verificación de identidad, hospedaje de lista de certificados revocados (LCR), entre otros.

Signatario: Significa la entidad que ha solicitado la emisión de un certificado dentro de la RPKI del PSC Proveedor de Certificados PROCERT, C.A. En estándar internacional el Signatario es el Suscriptor o parte que utiliza un certificado electrónico o recibe servicios de certificación electrónica.

SUSCERTE: Significa la Superintendencia de Servicios de Certificación Electrónica, que es el ente rector en materia de Certificación electrónica dentro de las organizaciones de gobierno en la República Bolivariana de Venezuela.

Uso del Certificado: Significa el conjunto de reglas que indican la aplicabilidad del certificado de una comunidad en particular y/o la clase de aplicación con requerimientos de seguridad comunes. Los usos del certificado se definen en el documento de la Política de Certificado PC.

Validación: Significa el proceso de verificación de la validez de un Certificado en términos de su estatus (Ej. suspendido o revocado).

1.6.1. Siglas.

AATL	Lista de confianza aprobada por Adobe
AC	Autoridad de Certificación
BR	Baseline Requirements
DNS	Servicio de Nombres de Dominio
DPC	Declaración de Prácticas de Certificación
DV	Dominio validado
ETSI	Instituto Europeo de Normas de Telecomunicación UE
ECDSA	algoritmo de curva elíptica
FIPS	Estándar Federal de Procesamiento de Información
FTP	Protocolo de transferencia de archivos
HSM	Módulo de seguridad de hardware
HTTP	Protocolo de transferencia de hipertexto
IETF	Grupo de Trabajo de Ingeniería de Internet
IGTF	Federación Internacional de Confianza en la Red
LCR	Lista de revocación de certificados
OID	Identificador de objeto
PC	Política de certificados
RFC	Solicitud de comentarios
SAN	Nombre alternativo del sujeto
SSL	Capa de sockets seguros
TLD	Dominio de nivel superior
	Seguridad de la capa de transporte
TSA	Autoridad de sellado de tiempo
TST	Token de marca de tiempo

TTL	Tiempo de vida
UIT	Unión Internacional de Telecomunicaciones
UTC	Tiempo Universal Coordinado
X.509	La norma UIT-T para certificados y su correspondiente marco de autenticación

2. Responsabilidades de publicación y repositorio.

2.1. Repositorios.

Según la CP, los certificados, las CRL y los objetos firmados por RPKI DEBEN ser disponibles para su descarga por parte de todos los usuarios de confianza, a fin de habilitarlos para validar estos datos. El PSC Proveedor de Certificados PROCERT, C.A. RPKI CA publicará certificados, CRL, y objetos firmados RPKI a través de un repositorio al que se puede acceder a través de la sección AC en la página web de PROCERT www.procert.net.ve en el enlace https://www.procert.net.ve/Internas/AC.aspx. Este repositorio se ajustará a la estructura descrita en [RFC6481].

2.2. Publicación de la información de certificación.

El PSC Proveedor de Certificados PROCERT, C.A. publicará certificados, CRL y RPKI emitidos por él a un repositorio que funciona como parte de un sistema distribuido por todo el mundo de repositorios RPKI. Los enlaces de publicación son los siguientes:

Por la Web.
CPS
https://www.procert.net.ve/Internas/AC.aspx.

PC
https://www.procert.net.ve/Internas/AC.aspx.

LCR

- PROCERT ECDSA SubCA
  - S/MIME CRL: www.procert.net.ve/ecc-crl/smime-ca.crl

OCSP

- PROCERT SubCA OCSP EDCSA
  - S/MIME OCSP: http://ocspsmime.procert.net.ve/ocsp

- SUSCERTE OCSP ECDSA
  http://ocsp-ecdsa.suscerte.gob.ve/

Certificados emitidos

- https://www.procert.net.ve/ConsultaPublica/index.aspx

Certificados de las CA

- PROCERT ECDSA
  - S/MIME cert: www.procert.net.ve/ecc-crt/smime-ca.crt

SUSCERTE certificado PSC PROCERT
EDCSA www.procert.net.ve/ecc-chain/cadena.p7b

Manejo ciclo de vida
https://www.procert.net.ve/sistemaAR/login.aspx . A través del Sistema AR el usuario está en capacidad de generar o revocar su certificado, siguiendo los pasos contenidos en el manual de usuario, al cual puede acceder a través de procert.net.ve/Docs/Proveedor de Certificados PROCERT ITFB, C.A. - Manual General de Usuario.pdf

Soporte
https://www.procert.net.ve/Internas/Soporte.aspx

Por email: soporte@procert.net.ve
Por teléfono: +58 (212]) 2674880
En persona: Multicentro Empresarial del Este, Núcleo B, Torre Libertador, Piso 13, oficina B-123, Municipio Chacao, Caracas, República Bolivariana de Venezuela.

2.3. Hora o frecuencia de publicación.
El PSC Proveedor de Certificados PROCERT, C.A. debe generar cada veinticuatro (24) horas una lista de certificados revocados (LCR), la cual se constituye en un mecanismo de validación y comprobación del estado de los certificados electrónicos y verificar cuales se encuentran revocados. Todo proceso de revocación de certificado es informado por PSC Proveedor de Certificados PROCERT, C.A., vía correo electrónico al Signatario. Dicha notificación se informa mensualmente a la SUSCERTE y se incluye en el depósito digitalizado mantenido por el PSC Proveedor de Certificados PROCERT, C.A.

El PSC Proveedor de Certificados PROCERT, C.A. CA publicará su LCR todos los días a las 14:00 horas GMT Caracas y es la nextUpdate LCR programada y emitida previamente por la CA de la RPKI del PSC Proveedor de Certificados PROCERT, C.A.

2.4. Controles de acceso en repositorios.
El acceso a los repositorios de confianza del PSC Proveedor de Certificados PROCERT, C.A. se ha configurado para que los Signatarios o usuarios de dichos repositorios puedan hacer solo consultas a los mismos, en el caso de los validadores de servicio tales como OCSP y LCR. Para el caso de consulta de cadenas de certificación se permite la descarga de estas y en el caso de documentación, igualmente se permite la descarga de los archivos y documentos requeridos y para su lectura. No están autorizados permiso de escritura, cambios en la información o ejecución de códigos a los fines de prevenir eventos de seguridad en contra de la RPKI.

3. Identificación y autenticación.
3.1. Nomenclatura.
3.1.1. Tipos de nombres.
El asunto de cada certificado emitido por esta organización es identificado por un nombre distintivo (DN) X.500. El nombre distintivo constará de un

único atributo Common Name (CN) con un valor generado por PSC Proveedor de Certificados PROCERT, C.A. El atributo serial number se incluye junto con el nombre común (para formar un conjunto de nombres distintivos relativos terminales), para distinguir entre instancias sucesivas de certificados asociados a la misma entidad.

3.1.2. Necesidad de que los nombres sean significativos.
El Proveedor de Certificados PROCERT, C.A. utiliza dentro de su estructura de certificados, nombres distintivos que permiten identificar tanto al Signatario o entidad usuaria que utiliza el certificado, como a la entidad emisora de dicho certificado, estableciéndose de esa manera la información que permita vincular a un emisor de certificados con sus Signatario o usuario finales.

3.1.3. Anonimato o seudónimo de los suscriptores.
Aunque los nombres de los sujetos en los certificados emitidos por esta organización NO DEBE ser significativo y puede parecer "aleatorio", el anonimato no es una función de esta RPKI; por lo tanto, el Proveedor de Certificados PROCERT, C.A. no emite certificados electrónicos S/MIME bajo anonimato o con seudónimos para entidades finales o signatarios.

3.1.4. Reglas para la interpretación de las distintas formas de nombre.
Las reglas de los nombres utilizados para la emisión de los certificados e identificación de los Signatarios o usuarios finales y el ente emisor serán las establecidas por el RFC 2253 y ITU-T X.500.

3.1.5. Unicidad de los nombres.
El Proveedor de Certificados PROCERT, C.A. certifica que los nombres de los sujetos son únicos entre los certificados que emite, al igual que sus números de serial, a los fines de hacer la diferenciación necesaria entre distintos Signatarios de la RPKI. La unicidad de nombres es aplicada dentro de la RPKI de Proveedor de Certificados PROCERT, C.A. de la siguiente manera:

- Certificados S/MIME: Identifica a una persona y permite igualmente firma electrónica, DEBE requerir para su emisión los nombres y apellidos propios, numero de identidad único y correo electrónico del Signatario, los cuales quedan asociados a un serial único de certificado de la RPKI. Para el momento de emisión de esta versión de DPC, el Proveedor de Certificados PROCERT, C.A. posee una SubCA S/MIME en operación.

3.1.6. Reconocimiento, autenticación y función de las marcas.
El Proveedor de Certificados PROCERT, C.A., solo emitirá certificados S/MIME pertenecientes a entidades jurídicas que no violen el derecho de propiedad sobre dominios debidamente registrados. No se verifica el derecho de uso de marca o nombre comercial o disputas existentes sobre dichas marcas; el Proveedor de Certificados PROCERT, C.A., solo verifica la veracidad de los documentos de empresa y propiedad de dominio, a los fines de la emisión de los certificados por la RPKI, luego de la validación y autorización por parte de la AR. El Proveedor de Certificados

PROCERT, C.A. no está obligado a emitir certificados cuando una entidad exista una disputa comercial de nombre y se reserva el derecho de revocar un certificado cuando exista una disputa comercial respecto al nombre comercial o dominio de empresa o entidad jurídica.

3.2. Validación inicial de la identidad.

El Proveedor de Certificados PROCERT, C.A., a los fines de cumplir con el estándar internacional y las leyes de la República Bolivariana de Venezuela, se encuentra en la obligación de ejecutar un examen riguroso de la información que es suministrada por los Signatario o usuario finales de certificados electrónicos o servicios de certificación; en tal sentido la AR de Proveedor de Certificados PROCERT, C.A., utiliza todos los medios legales y enlaces gubernamentales o no, que sean públicos y que permitan establecer la idoneidad y legalidad de la información suministrada por los Signatarios o usuarios finales de certificados electrónicos o servicios de certificación, durante el proceso de contratación de los mismos, a los fines de generar las consecuencias legales y el no repudio.

3.2.1. Método para probar la posesión de una clave privada.

Los Signatarios que utilizan certificados electrónicos generados por Proveedor de Certificados PROCERT, C.A., deben cumplir un proceso de validación de identidad que debe ser positivo en cuando a la validación de información suministrada y previo al proceso de generación de su par de claves criptográficas. La generación de la clave privada varia en cada caso, pero siempre validando que sea el usuario final propietario del certificado, quien genera y administra su certificado. Los métodos de validación de posesión de identidad de una clave privada en Proveedor de Certificados PROCERT, C.A., son los siguientes:

- Certificado S/MIME: El Signatario o usuario final suministra toda la información requerida para su validación de identificación; dicha información se registra en la plantilla de certificado correspondiente y una vez cumplidos los pasos de aprobación de la AR; el Signatario desde el portal de Proveedor de Certificados PROCERT, C.A., procederá a la generación del par de claves criptográficas de su certificado. Generada la petición la AC de Proveedor de Certificados PROCERT, C.A., procede a la aprobación del certificado y el usuario descargara su certificado incluyendo una clave de seguridad para administrar la firma de su certificado demostrando la prueba de posesión (PoP) de la clave privada correspondiente a la clave pública del certificado. En el sistema de firma en línea, la firma electrónica se administra con un usuario y clave de acceso al portal, más una clave única de un solo tiempo que llega al Signatario por medio de correo electrónico o mensaje de texto SMS, demostrando de esa manera la prueba de posesión (PoP) de la clave privada correspondiente a la clave pública del certificado.

3.2.2. Autenticación de la identidad de la organización.

Proveedor de Certificados PROCERT, C.A., a través de la AR ejecuta la validación de identidad y la verificación de todos los datos aportados por los Signatarios y entidades finales que utilizan certificados electrónicos generados por la RPKI.

- Los certificados S/MIME bajo la legislación de la República Bolivariana de Venezuela, en cumplimiento del estándar internacional, dependiendo del certificado que se gestione y luego de ser efectuada de manera conforme la validación de identidad y la documentación aportada por el Signatario por parte de la AR; acreditan la identidad del Signatario o usuario final del certificado, su afiliación de determinado gremio o entidad y otorgan el no repudio de las transacciones efectuadas por el Signatario que se trate. Los datos e información suministrada por el Signatario se resguardan con criterio de confidencialidad. La verificación de la información se efectúa por la AR contra fuentes gubernamentales a los fines de establecer la certeza de los datos suministrados por los Signatario y por ende acreditar su identidad.

  Proveedor de Certificados PROCERT, C.A., dentro de los elementos de verificación que ejecuta la AR, contempla la verificación tanto de la procesión del dominio como del correo electrónico incluyendo el uso de correo electrónico seguro dentro de los atributos del certificado electrónico. Los correos electrónicos que identifiquen a un Signatario no podrán ser o contener definiciones generales y deberán identificar claramente a los signatarios con su nombre y apellido. Se incluye un mecanismo de validación de propiedad y control de la dirección de correo electrónico que el Signatario debe completar de forma exitosa a satisfacción de la AR, sin lo cual no será emitido el certificado electrónico.

  Sin embargo, los certificados son emitidos por la RPKI a los Signatarios de una manera que preserve la exactitud de la distribuciones de INR representadas en Proveedor de Certificados PROCERT, C.A. Adicionalmente Proveedor de Certificados PROCERT, C.A., posee en su portal web el siguiente enlace https://www.procert.net.ve/ConsultaPublica/index.aspx, a través del cual, cualquier entidad o persona podrá determinar si un certificado electrónico emitidos por Proveedor de Certificados PROCERT, C.A., pertenece a un Signatario determinado.

3.2.3. Autenticación de la identidad individual.

Proveedor de Certificados PROCERT, C.A., a los fines de gestionar y emitir un certificado electrónico de persona o entidad, ejecuta procedimientos de validación de información e identidad a través de la AR; dichos procedimientos son los siguientes:

- Certificados S/MIME.
  - Nombres y apellidos del Signatario
  - Teléfono de contacto del Signatario (Móvil o fijo)
  - Correo electrónico del Signatario.
  - Validación de control y propiedad del correo electrónico a través de un proceso de confirmación de cuenta de correo electrónico.
  - Copia digitalizada del documento de identidad.
  - Revisión del documento de identidad del Signatario a los fines de certificar que se trata de una persona debidamente registrada en el servicio nacional de identidad.

- Copia digitalizada del Registro de Información Fiscal (RIF) Tributario del Signatario.
- Revisión del RIF del Signatario a los fines de certificar su validez y existencia.
- Recibo de servicio público donde se figure la dirección de domicilio del Signatario.
- Video de identificación del Signatario indicando su intención de contratar un certificado electrónico.
- En caso de ser profesional acompañar los comprobantes de inscripción en Colegios Profesionales.
- Entrevista de validación de identidad en caso de ser considerado por la AR.

- Certificados S/MIME para representante de empresa.
  - Nombres y apellidos del Signatario
  - Teléfono de contacto del Signatario (Móvil o fijo)
  - Correo electrónico del Signatario.
  - Validación de control y propiedad del correo electrónico a través de un proceso de confirmación de cuenta de correo electrónico.
  - Copia digitalizada del documento de identidad.
  - Revisión del documento de identidad del Signatario a los fines de certificar que se trata de una persona debidamente registrada en el servicio nacional de identidad.
  - Copia digitalizada del Registro de Información Fiscal (RIF) Tributario del Signatario.
  - Revisión del RIF del Signatario a los fines de certificar su validez y existencia.
  - Recibo de servicio público donde se figure la dirección de domicilio del Signatario.
  - Video de identificación del Signatario indicando su intención de contratar un certificado electrónico.
  - En caso de ser representante de empresa o funcionario público acompañar los documentos que acrediten su representación (Acta, poder o Estatutos) o las Gacetas Oficiales de designación en cargo.
  - Entrevista de validación de identidad en caso de ser considerado por la AR.
  - Datos del documento constitutivo o de creación de la entidad jurídica que representa y su condición y cargo.
  - Copia digitalizada del Registro de Información Fiscal (RIF) Tributario del Signatario.
  - Revisión del RIF la entidad jurídica que representa a los fines de certificar su validez y existencia.
  - Recibo de servicio público donde se figure la dirección de domicilio la entidad jurídica.
  - Recibo de servicio público donde se figure la dirección de domicilio de la entidad jurídica.

3.2.4. Información no verificada del suscriptor.

Proveedor de Certificados PROCERT, C.A., no se incluyen datos de suscriptores no verificados en los certificados emitidos bajo esta política de

certificados, incluso para el acceso a la información del sujeto (SIA) [RFC6487].

3.2.5. Validación de la autoridad.
Como se ha establecido en el punto 3,2,3, que precede, la AR de Proveedor de Certificados PROCERT, C.A., una vez cuente con la información y documentación solicitada al Signatario o entidad final usuaria del certificado, la AR procederá a validar la misma contra registros públicos de gobierno e independientes a los fines de contratar su validez y establecer los mecanismos de verificación de control de correo electrónico, teléfono y dominio. En los casos en que la validación resulte exitosa, se procederá con la tramitación del certificado electrónico. En los casos que ocurran objeciones a la documentación o en el proceso de comprobación de control de correo electrónico, teléfono y dominio, no se tramitará la generación del certificado hasta tanto sean subsanadas las observaciones y no conformidades.

3.2.6. Criterios de interoperabilidad.
Proveedor de Certificados PROCERT, C.A., no posee actualmente CA subordinadas o un esquema de certificación cruzada con otras CA. No obstante, lo anterior, declara que está en capacidad de establecer esos esquemas de operación, los cuales mediarán a través de acuerdos suscritos y autorizados por la SUSCERTE para los casos de operación dentro de la República Bolivariana de Venezuela.

3.3. Identificación y autenticación para solicitudes de cambio de clave.

3.3.1. Identificación y autenticación para la reintroducción rutinaria de claves.
Proveedor de Certificados PROCERT, C.A. mantiene una política de no remisión de claves para los certificados S/MIME. En los casos que este comprometida la clave o se requiera un nuevo certificado el Signatario debe hacer una nueva solicitud que deberá ser validada a los fines de poder ser emitido el certificado, descontándose el período de vigencia del certificado en el nuevo proceso de emisión.

3.3.2. Identificación y autenticación para la reintroducción de la clave después de la revocación.
Proveedor de Certificados PROCERT, C.A. mantiene una política de no remisión de claves para los certificados S/MIME. En este caso se procede como se indicó en el punto 3.3.1. En el caso de los certificados igualmente aplica el procedimiento indicado en el punto 3.3.1.

3.4. Identificación y autenticación para la solicitud de revocación.
Proveedor de Certificados PROCERT, C.A., mantiene un esquema de operación y gestión, donde el Signatario o entidad final usuaria de un certificado electrónico generado por RPKI de Proveedor de Certificados PROCERT, C.A., gestiona directamente el proceso de revocación de su propio certificado electrónico; en este caso el certificado S/MIME podrá ser revocado siguiendo los pasos siguientes:

- El Signatario o representante autorizado debe ingresar en el sistema AR introduciendo su nombre de usuario y contraseña.

- El Signatario o representante autorizado debe ingresar en la sección de revocación del certificado e indicar la razón por la cual revoca su certificado. El sistema emitirá un correo de alerta a la dirección de correo electrónico registrada indicando el inicio del proceso de revocación.
- Seguidamente el Signatario o representante autorizado debe ingresar la clave de un solo tiempo (OTP) que es enviada al teléfono asociado a su cuenta. Si supera con éxito este proceso se activará el botón de revocación.
- Activado el botón de revocación el Signatario o representante autorizado procederá a revocar el certificado.
- El sistema AR enviará un correo electrónico a la AR para informar acerca de la revocación del certificado electrónico.

4. Requisitos operativos del ciclo de vida del certificado.

4.1. Solicitud de certificado.

4.1.1. Quién puede presentar una solicitud de certificado.

Cualquier suscriptor al día que posea INR distribuidos por Proveedor de Certificados PROCERT, C.A., puede presentar una solicitud de certificado a esta CA. (El significado exacto de "al día" está de acuerdo con el Política de Proveedor de Certificados PROCERT, C.A. Todo Signatario o representante de entidad final usuaria de certificado deberá cumplir con la entrega de la documentación y los pasos de validación establecidos por la AR de Proveedor de Certificados PROCERT, C.A., sin lo cual no se dará trámite a su solicitud.

4.1.2. Proceso de inscripción y responsabilidades.

Los signatarios y entidades finales interesados en obtener certificados electrónicos de la RPKI de Proveedor de Certificados PROCERT, C.A., deben ingresar a la URL www.procert.net.ve y acceder al sistema AR a través de procert.net.ve/sistemaAR/login.aspx y gestionar su registro en caso de no contar con certificados electrónicos. En el proceso de registro se deben cumplir los siguientes pasos:

- El Signatario se registra en el sistema AR y El signatario seleccionará el tipo de certificado electrónico que genera la CA de Proveedor de Certificados PROCERT, C.A.
- EL Signatario debe acompañar la documentación exigida para cada certificado S/MIME.
- El Signatario debe subir la documentación en formato PDF y un video de identidad y validación de uso del certificado.

Toda persona o empresa que reúna las condiciones legales aporte la documentación y requisitos legales y técnicos, superando el proceso de validación de la AR podrá optar a un certificado electrónico emitido por la RPKI de Proveedor de Certificados PROCERT, C.A.

4.2. Tramitación de la solicitud de certificado.

La AR de Proveedor de Certificados PROCERT es la encargada de construir el expediente electrónico del Signatario a los fines de incluir en el mismo los requisitos normativos y legales exigidos dentro y fuera de la República Bolivariana de Venezuela, para la emisión conforme del tipo de certificado que solicita el Signatario y Proveedor de Certificados PROCERT, C.A., está en capacidad de

ofrecer. Una vez validado el expediente de cada Signatario y estando conforme los procesos de revisión de documentación y validación de identidad, el sistema AR enviará al Signatario un correo electrónico indicando que puede generar su petición de certificado o cargar su CSR según se trate del tipo de certificado que el Signatario gestiona.

4.2.1. Realización de funciones de identificación y autenticación.

La AR de Proveedor de Certificados PROCERT, C.A., luego de recibidos los documentos y soportes entregados por los Signatarios o entidades finales usuarias de certificados electrónicos, en cumplimiento de las normas internacionales y legales aplicables dentro de la República Bolivariana de Venezuela, procederá a su revisión, a los fines de constatar y dejar constancia de las declaraciones y documentación aportada por los Signatarios o entidades finales usuarias de certificados electrónicos; dicho proceso se efectuará de la siguiente manera:

- Certificados S/MIME: La AR de Proveedor de Certificados PROCERT, C.A., procede a validar la identificación y el Registro de Información Fiscal (RIF) que son aportada por el Signatario a través de sistemas que se encuentran integrados al Sistema Nacional Integrado de Administración Aduanera y Tributaria (SENIAT), Concejo Nacional Electoral (CNE) y el Servicio Administrativo de Identificación, Migración y Extranjería (SAIME); a los fines de determinar su validez y exactitud de dicha información. Igualmente y en caso de que las direcciones de correo correspondan a personas jurídicas, se valida la existencia de los dominios a través del uso de la información suministrada por https://whois.domaintools.com/ Whois Lookup, Domain Availability & IP Search - DomainTools, ICANN Lookup y NIC.ve . Los dominios de las empresas son validados y se solicita una carta del representante de recursos humanos de la empresa a los fines de dejar constancia que el Signatario labora para dicha empresa; en el caso de representantes de empresa se solicitan los documentos poderes, actas o registros que acrediten su representación de empresa y en el caso de funcionarios públicos, se solicita adicionalmente la Gaceta Oficial en donde figure su designación y cargo. Las direcciones de correo de Gmail son validadas a los efectos de verificar su existencia y control sobre las mismas y solo son aceptadas para certificados de persona natural. La dirección física del Signatario se valida contra los registros oficiales aportados y un recibo de servicio público aportado por el Signatario y que se requiere para gestionar su certificado.

- Certificados SSL: La AR de Proveedor de Certificados PROCERT, C.A., procede a validar la identificación y el Registro de Información Fiscal (RIF) que son aportada por el Signatario o representante de la entidad final usuaria del certificado electrónico, a través de sistemas que se encuentran integrados al Sistema Nacional Integrado de Administración Aduanera y Tributaria (SENIAT) y el Servicio Administrativo de Identificación, Migración y Extranjería (SAIME); a los fines de determinar su validez y exactitud de dicha información. Igualmente y en caso de que las direcciones de correo correspondan a personas jurídicas, se valida la existencia de los dominios a través del uso de la

información suministrada por https://whois.domaintools.com/ Whois Lookup, Domain Availability & IP Search - DomainTools, ICANN Lookup y NIC.ve . Los dominios de las empresas son validados y se solicita una carta del representante de informática de la empresa a los fines de dejar constancia que el dominio les pertenece y están en proceso de gestión del certificado indicando su uso; los representantes de empresa deben acompañar los documentos poderes, actas o registros que acrediten su representación de empresa y en el caso de funcionarios públicos, se solicita adicionalmente la Gaceta Oficial en donde figure su designación y cargo. La dirección física del Signatario se valida contra los registros oficiales aportados y un recibo de servicio público aportado por el Signatario y que se requiere para gestionar su certificado.

4.2.2. Aprobación o denegación de solicitudes de certificado.

Proveedor de Certificados PROCERT, C.A., establece que todas aquellas solicitudes de certificados hechos por Signatarios o entidades finales usuarias de certificados serán procesadas y aprobadas siempre y cuando se cumpla de forma satisfactoria el proceso de validación descrito en 4.2.1. por parte de la AR sobre la documentación, recaudos y validaciones que debe cumplir el Signatario o entidad final usuaria de certificados electrónicos. Sin excepción, no serán tramitadas las solicitudes de certificados que no cumplan los requisitos establecidos por Proveedor de Certificados PROCERT, C.A. y que se fundamentan en normas y estándares nacionales e internaciones que regulas la actividad de RPKI.

4.2.3 Plazo de tramitación de las solicitudes de certificado

Proveedor de Certificados PROCERT, C.A., establece un proceso máximo de cuarenta y ocho (48) horas para la emisión de los certificados electrónicos una vez los Signatarios o entidades finales usuarias de certificados electrónicos hayan cumplido y superado de forma satisfactoria para la AR de Signatario o entidad final usuaria de certificados electrónicos. todos los procesos contemplados en 4.2.1.

4.3. Emisión de certificados

4.3.1. Acciones de CA durante la emisión de certificados

La CA de Proveedor de Certificados PROCERT, C.A., solo validará y gestionará aquellas solicitudes de certificados electrónicos que superen el proceso de validación y comprobación de la AR de Proveedor de Certificados PROCERT, C.A. Una vez aprobada la solicitud de certificado electrónico por parte del Signatario o entidad final usuaria del certificado electrónico, la AR aprobará el trámite e inmediatamente el Sistema AR de Proveedor de Certificados PROCERT, C.A, activará el botón de generación de petición de certificado; seguidamente el Signatario pulsará el botón de generación de solicitud de certificado y el Sistema AR enviará su solicitud de certificado a la CA de Proveedor de Certificados PROCERT, C.A. El operador de la CA de Proveedor de Certificados PROCERT, C.A verificará la información que contendrá el certificado a los fines del cumplimiento del estándar nacional e internacional y procederá a pulsar el botón de aprobación de la solicitud del certificado; seguidamente la CA

emitirá el certificado e informará vía correo electrónico al Signatario acerca de la emisión de su certificado.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado
Proveedor de Certificados PROCERT, C.A. notifica de forma automatizada al Signatario vía correo electrónico acerca de la aprobación de su certificado. El signatario debe ingresar al Sistema AR de Proveedor de Certificados PROCERT, C.A., acceder la sección descarga de certificado, colocar la clave de acceso a esa sección y tendrá a la vista por una sola vez la clave privada de su certificado, la cual requiere para exportarlo de forma segura, siguiendo el procedimiento establecido por Proveedor de Certificados PROCERT, C.A. e incluyendo una clave para el uso de su certificado desde su equipo. Adicionalmente el usuario podrá firmar en línea con su certificado usando el Sistema AR de Proveedor de Certificados PROCERT, C.A. e incluyendo los factores de autenticación de dos factores que le son presentados, sin lo cual no podrá firmar. En el caso de los certificados SSL. Los usuarios finales del certificado electrónico recibirán el certificado con la cadena de certificación vía correo electrónico con las instrucciones de instalación correspondiente.

4.3.3. Notificación de la emisión de certificados por parte de la CA a otras entidades.
Proveedor de Certificados PROCERT, C.A. debe notificar a la SUSCERTE mediante un reporte mensual, acerca de los certificados electrónicos que ha emitido durante el mes inmediato anterior al de la fecha del reporte.

4.4. Aceptación del certificado

4.4.1. Conducta que constituye la aceptación del certificado
Cuando se emite un certificado, la CA de Proveedor de Certificados PROCERT, C.A. procede a la publicación en su repositorio de certificados emitidos Consulta Pública (procert.net.ve) para que puedan ser consultados por terceros interesados y notifica directamente y por correo electrónico al Signatario o usuario final de certificado. Una vez emitidos, los Signatarios o entidades finales usuarias de los certificados procederán a instalarlos en sus equipos y administrar con los mecanismos de seguridad que poseen y ofrece el Sistema AR para los certificados S/MIME el proceso de firma.

4.4.2. Publicación del certificado por parte de la CA
Los certificados se publicarán Consulta Pública (procert.net.ve), siguiendo la conducta descrita en la sección 4.4.1. La publicación será efectuada dentro de las cuarenta y ocho (48) horas siguientes a la validación satisfactorias por parte de la AR.

4.4.3. Notificación de la emisión de certificados por parte de la CA a otras entidades.
Proveedor de Certificados PROCERT, C.A. debe notificar a la SUSCERTE mediante un reporte mensual, acerca de los certificados electrónicos que ha emitido durante el mes inmediato anterior al de la fecha del reporte.

4.5. Uso de pares de claves y certificados.
Proveedor de Certificados PROCERT, C.A. procede a informa a los Signatarios, entidades finales usuarias de los certificados electrónicos y terceras partes interesadas acerca del uso de los certificados electrónicos y de las responsabilidades derivadas de dicho uso.

4.5.1. Uso de la clave privada y el certificado del suscriptor.
Los certificados emitidos por Proveedor de Certificados PROCERT, C.A. al INR subordinado y sus titulares son certificados de CA. La clave privada y pública asociada a cada uno de los estos certificados se utiliza conforme al uso establecido en el uso establecido y uso mejorado de cada certificado, los cuales se encuentran descritos en la CP de Proveedor de Certificados PROCERT, C.A.

4.5.2. Uso de certificados y claves públicas de usuario de confianza.
Los usuarios de confianza principales de esta RPKI son las organizaciones que usan los certificados electrónicos generados por la CA de Proveedor de Certificados PROCERT, C.A. y que establecen la confianza en el uso del certificado que cumplan con X.509, IETF RFC y otros estándares aplicables en materia de RPKI y AR y con el estándar internacional establecido por el CA Browser Fórum, las normas dictadas por la SUSCERTE y la legislación que regula la materia dentro de la República Bolivariana de Venezuela.

En todo caso los usuarios deben confiar de los certificados que una vez comprobados a través de la LCR o el servicio OCSP permitan establecer que son válidos y están vigentes y que todas las firmas efectuadas en el período de vigencia de dicho certificado se entenderán como válidos y gozaran del No repudio, integridad y prueba legal. Las condiciones de uso de los certificados emitidos por la RPKI de Proveedor de Certificados PROCERT, C.A. se encuentran descritas en la PC y deben ser revisadas por los Signatarios a los fines de conocer su alcance y uso. Adicionalmente el contrato y términos de uso de los certificados establecen la obligación de los Signatarios respecto al uso de los certificados electrónico.

4.6. Renovación del certificado.
4.6.1. Circunstancia para la renovación del certificado.
Proveedor de Certificados PROCERT, C.A. informa a todos los Signatarios o entidades finales usuarias de certificados electrónicos S/MIME que las circunstancias que aplican para optar a la renovación de un certificado electrónico emitido por la RPKI es el vencimiento del del período de vigencia o el compromiso de la clave privada del certificado electrónico. En ambos supuestos se procederá siempre a la generación de un nuevo par de claves y como se indica en el numeral 4.7. La AR de Proveedor de Certificados PROCERT, C.A. notifica con treinta (30) días de anticipación a sus Signatarios, respecto al vencimiento del certificado. Para los certificados SSL se procederá a la presentación de un nuevo CSR. En ambos casos aplica el proceso previo de validación de la AR, sin lo cual no serán emitidos certificados.

4.6.2. Quién puede solicitar la renovación.

El Signatario o entidades finales usuarias de certificados electrónicos puede iniciar el proceso de renovación de su certificado electrónico. La AR de Proveedor de Certificados PROCERT, C.A. validará la identidad y documentación que debe presentar el Signatarios o entidades finales usuarias de certificados electrónicos y se procederá conforme se indicó en el punto 4.2.1. de esta DPC.

4.6.2. Tramitación de solicitudes de renovación de certificados.

Las solicitudes de renovación de certificados serán gestionadas por el mismos Signatario a través del portal de Signatarios o entidades finales usuarias de certificados electrónicos www.procert.net.ve y seleccionar el enlace del sistema AR a través de procert.net.ve/sistemas/login.aspx y procederá a incluir y consignar la información que le sea requerida conforme al con X.509, IETF RFC y otros estándares aplicables en materia de RPKI y AR y con el estándar internacional establecido por el CA Browser Fórum, las normas dictadas por la SUSCERTE y la legislación que regula la materia dentro de la República Bolivariana de Venezuela. La verificación de toda esa información y de la entidad del Signatario o usuario final del certificado electrónico será ejecutada de conformidad con lo indicado en el punto 4.2.1. que precede.

4.6.4. Notificación de la emisión de un nuevo certificado al abonado.

Proveedor de Certificados PROCERT, C.A. notifica de forma automatizada al Signatario vía correo electrónico acerca de la aprobación de su certificado. Esta notificación se efectuará conforme a lo indicado en el punto 4.3.2.

4.6.5. Conducta constitutiva de aceptación de un certificado de renovación.

Se entenderá como proceso de aceptación el contemplado y descrito en el aparte 4.4.1. de esta DPC.

4.6.6. Publicación del certificado de renovación por parte de la CA.

Véase la sección 4.4.2.

4.6.7. Notificación de la emisión de certificados por parte de la CA a otras entidades.

Véase la sección 4.4.3.

4.7. Cambio de clave del certificado.

4.7.1. Circunstancia para la reintroducción de la clave del certificado.

Proveedor de Certificados PROCERT, C.A. no renueva claves. En caso de ser requerida la emisión de un nuevo certificado electrónico, la misma solo podrá proceder bajo la ocurrencia de los siguientes supuestos:

- Compromiso de la clave privada.
- Vencimiento del período de vigencia del certificado.

La verificación de toda esa información y de la entidad del Signatario o usuario final del certificado electrónico será ejecutada de conformidad con lo indicado en el punto 4.2.1. que precede.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública.
Solo el titular de un certificado puede solicitar una nueva clave. Además Proveedor de Certificados PROCERT, C.A. inicia una nueva clave basada en una notificación validada de compromiso de clave o vencimiento. Si el signatario o entidad final usuaria del certificado electrónico, solicita un nuevo certificado deberá cumplir los pasos previstos y contenidos dentro del aparte 4.2. de esta DPC. No obstante, el Sistema AR de Proveedor de Certificados PROCERT, C.A. permite al Signatario gestionar el ciclo de vida de su certificado y proceder a la revocación del certificado si así lo considera necesario, indicando a tales efectos la causa de la revocación. Las solicitudes que no sean autogestionadas serán validadas por la AR de Proveedor de Certificados PROCERT, C.A., requiriendo la aprobación de la AR para proceder a la revocación.

4.7.3. Procesamiento de solicitudes de cambio de clave de certificados.
Proveedor de Certificados PROCERT, C.A. no renueva claves. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.7.4. Notificación de la emisión de un nuevo certificado al suscriptor.
Proveedor de Certificados PROCERT, C.A. notifica de forma automatizada al Signatario vía correo electrónico acerca de la aprobación de su certificado. Esta notificación se efectuará conforme a lo indicado en el punto 4.3.2.

4.7.5. Conducta que constituye la aceptación de un certificado con nueva clave.
Cuando se emite un nuevo certificado la CA lo publicará en el archivo en los repositorios indicados y conforme a lo establecido en el punto 4.4.1 de esta DPC.

4.7.6. Publicación del certificado de nueva clave por parte de la CA.
Proveedor de Certificados PROCERT, C.A. no renueva claves. Para conocer el proceso de publicación de un certificado por la CA ver el aparte 4.4.2. de esta DPC.

4.7.7. Notificación de la emisión de certificados por parte de la CA a otras entidades.
Proveedor de Certificados PROCERT, C.A. debe notificar a la SUSCERTE mediante un reporte mensual, acerca de los certificados electrónicos que ha emitido durante el mes inmediato anterior al de la fecha del reporte.

4.8. Modificación del certificado.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario

debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.1. Circunstancia para la modificación del certificado.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.2. Quién puede solicitar la modificación del certificado.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.3. Procesamiento de solicitudes de modificación de certificados.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.4. Notificación de la emisión de certificados modificados al suscriptor.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.5. Conducta que constituye la aceptación del certificado modificado.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.6. Publicación del certificado modificado por parte de la CA.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2.

4.8.7. Notificación de la emisión de certificados por parte de la CA a otras entidades.
Proveedor de Certificados PROCERT, C.A. no modifica certificados. En caso de ser requerida la emisión de un nuevo certificado electrónico, el Signatario debe cumplir a cabalidad cada uno de los pasos y procesos contemplados en el aparte 4.2. Proveedor de Certificados PROCERT, C.A. debe notificar a la SUSCERTE mediante un reporte mensual, acerca de los certificados electrónicos que ha emitido durante el mes inmediato anterior al de la fecha del reporte.

4.9. Revocación y suspensión del certificado.

La revocación de un certificado es el proceso que pone fin a la vida útil del certificado y su uso conforme invalidándolo, de esa manera otros Signatarios no deben confiar en ese certificado. La CA de Proveedor de Certificados PROCERT, C.A. coloca en la LCR a los certificados que son revocados, a los fines de mantener la confianza de los Signatarios. Igualmente, la RPKI de Proveedor de Certificados PROCERT, C.A. mantiene el OCSP para que los Signatarios, terceros interesados o sistemas de información puedan validar en línea si un certificado se encuentra revocado, aumentando de esa manera la confianza en el uso de los certificados electrónicos. Para revocar un certificado el Signatario titular del certificado debe solicitarlo a la AR de Proveedor de Certificados PROCERT, C.A. La suspensión es el proceso mediante el cual se modifica la validez temporal de un certificado electrónico y solo puede ser solicitada por el Signatario titular del certificado electrónico. La AR de Proveedor de Certificados PROCERT, C.A. previa verificación, procede a colocar un certificado fuera de uso por un período de tiempo determinado, pudiendo ser activado nuevamente luego de vencido el lapso de suspensión.

4.9.1. Circunstancias para la revocación.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional establece que la solicitud de revocación del certificado cuando no es efectuada directamente por el Signatario en el Sistema AR, solo puede ser tramitada por el Signatario ante la AR de Proveedor de Certificados PROCERT, C.A. y basada en uno de los siguientes supuesto:

- Compromiso de la clave privada del certificada.
- Vencimiento del período de vigencia del certificado.
- Renovación del certificado.
- Solicitud del Signatario de un nuevo certificado por actualización o cambio de uso conforme a lo establecido en la PC.
- Solicitud Judicial.
- Fallecimiento del Signatario.
- Desincorporación del Signatario de la entidad jurídica que representa.
- Compromiso o perdida del dispositivo o medio de almacenamiento del certificado.
- Cambio o modificación del estándar internacional y nacional que hagan necesaria le revocación del certificado.

4.9.2. Quién puede solicitar la revocación.

Solo el Signatario o entidades finales propietarias de los certificados electrónicos emitidos por la RPKI de Proveedor de Certificados PROCERT, C.A., pueden iniciar el proceso de revocación de su certificado electrónico. La AR de validará la identidad y documentación que debe presentar el Signatario o entidades finales usuarias de certificados electrónicos y se procederá a la revocación del certificado. De igual manera el Signatario o entidades finales propietarias de los certificados electrónicos, podrán, ingresando y cumpliendo los pasos de autenticación y colocando la clave de seguridad de un solo tiempo (OTP), necesarias para autorizar la transacción dentro del Sistema AR y proceder a revocar en línea su certificado.

4.9.3. Procedimiento para la solicitud de revocación.

El Signatario o entidades finales propietarias de los certificados electrónicos emitidos por la RPKI de Proveedor de Certificados PROCERT, C.A., cuando soliciten la revocatoria de su certificado, deben enviar su solicitud en correo firmado electrónicamente, a través de su cuenta de correo electrónico registrada en Proveedor de Certificados PROCERT, C.A. La solicitud debe estar fundamentada en una de las causales establecidas en el aparte 4.9.1. Recibida la solicitud la AR validará la identidad y documentación que debe presentar el Signatario o entidades finales usuarias de certificados electrónicos y se procederá a la revocación del certificado. Se informará vía correo electrónico acerca de la revocación del certificado. De igual manera el Signatario o entidades finales propietarias de los certificados electrónicos, podrán, ingresando y cumpliendo los pasos de autenticación y colocando la clave de seguridad de un solo tiempo (OTP), necesarias para autorizar la transacción dentro del Sistema AR y proceder a revocar en línea su certificado.

4.9.4. Período de gracia de la solicitud de revocación.

El Signatario o entidades finales propietarias de los certificados electrónicos emitidos por la RPKI de Proveedor de Certificados PROCERT, C.A., deben solicitar la revocatoria de su certificado, dentro de las veinticuatro (24) horas siguientes a la ocurrencia de alguna de las causales de revocación indicadas en el aparte 4.9.1.

4.9.5. Plazo dentro del cual la CA debe procesar la solicitud de revocación.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional establece que la solicitud de revocación del certificado cuando es efectuada a través de correo electrónico soporte@procert.net.ve serán tramitadas dentro de la una (1) hora siguiente a la validación por parte de la AR. De igual manera el Signatario o entidades finales propietarias de los certificados electrónicos, podrán, ingresando y cumpliendo los pasos de autenticación y colocando la clave de seguridad de un solo tiempo (OTP), necesarias para autorizar la transacción dentro del Sistema AR y proceder a revocar en línea su certificado.

4.9.6. Requisito de comprobación de revocación para las partes que confían en la confianza.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional X.509, IETF RFC y del RFC 6484 establece dentro de su RPKI dos (2) métodos de comprobación del estado de los certificados emitidos por la CA de Proveedor de Certificados PROCERT, C.A.; el primero es la Lista de Certificados Revocados (LCR), el cual consiste en una publicación periódica de los certificados que son revocados a los fines de hacerlo público y generar mayor confianza en los Signatarios de la RPKI. El segundo método de comprobación del estado del certificado es el Online Certifícate Status Protocol (OCSP) el cual permite validar en línea el estado de un certificado y comprobar si está revocado. El enlace a la LCR de Proveedor de Certificados PROCERT, C.A. es la siguiente: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl.; el enlace para el OCSP es el siguiente: S/MIME: http://ocspsmime.procert.net.ve/ocsp

4.9.7. Frecuencia de emisión de CRL.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional X.509, IETF RFC y del RFC 6484 establece dentro de su RPKI un esquema periódico de publicación de la LCR de la CA de Proveedor de Certificados PROCERT, C.A. La publicación de las LCR se ejecuta cada veinticuatro (24) horas y está disponible al público en general a través de los enlaces: S/MIME: http://www.procert.net.ve/ecc-crl/smime-ca.crl.

4.9.8. Latencia máxima para CRL.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional X.509, IETF RFC y del RFC 6484 establece dentro de su RPKI un período de latencia en la publicación de la LCR de quince (15) minutos luego de ser generada y hasta ser colocadas en el repositorio.

4.10. Servicios de estado de certificados.

Proveedor de Certificados PROCERT, C.A. en cumplimiento del estándar internacional X.509, IETF RFC y del RFC 6484 establece dentro de su RPKI un método de comprobación del estado del certificado en línea que se denomina Online Certifícate Status Protocol (OCSP) el cual permite validar en tiempo real el estado de los certificados electrónicos emitidos por la CA de Proveedor de Certificados PROCERT, C.A. El OCSP arroja tres respuestas a las consultas que deben ser ejecutadas y que se pueden efectuar a través del enlace http://ocspsmime.procert.net.ve/ocsp. Las respuestas que genera el OCSP respecto al estado de los certificados electrónicos generados por la CA de Proveedor de Certificados PROCERT, C.A. son las siguientes:

- Válido**:** El certificado está vigente y no ha sido revocado.
- Revocado**:** El certificado ha sido revocado y no debe confiarse en él.
- Desconocido**:** El servidor OCSP no tiene información sobre el estado del certificado.

El servicio de consulta OCSP dentro de la RPKI de Proveedor de Certificados PROCERT, C.A. se encuentra debidamente publicado y disponible de forma permanente.

5. Controles de instalaciones, gestión y operaciones.

5.1. Controles físicos.

Proveedor de Certificados PROCERT, C.A. presta sus servicios de RPKI basado en una plataforma tecnológica instalada en centros de datos que poseen mecanismos y controles de seguridad, operación y acceso controlado que permiten ofrecer a los Signatarios o entidades finales usuarias de certificados electrónicos la confianza necesaria en los mismos. Todas las medidas implantadas para la RPKI de Proveedor de Certificados PROCERT, C.A. están orientadas a la continuidad de negocios y recuperación ante desastres, garantizar la seguridad lógica y física de los equipos y personal que conforman la RPKI y la disuasión contra acciones que pretendan afectar el desempeño esperado de la RPKI.

5.1.1. Ubicación y construcción del sitio.

Proveedor de Certificados PROCERT, C.A. opera su RPKI desde centros de datos que poseen categoría TIER 3 y 4 asegurando de esa manera

altos entandares de operación y desempeño que permiten establecer la confianza de los Signatarios en el debido funcionamiento de los certificados electrónicos. Los centros de datos que utiliza Proveedor de Certificados PROCERT, C.A. se encuentran dentro de la República Bolivariana de Venezuela. El centro de datos desde donde opera Proveedor de Certificados PROCERT, C.A. mantiene las pólizas o instrumentos emitidos por empresas de seguros solventes y reconocidas, a los efectos de mantener un respaldo en caso de ocurrencia de una contingencia que afecta la integridad física de la referida sede administrativa y pueda ofrecer de esa manera una garantía de su continuidad operacional. Proveedor de Certificados PROCERT, C.A. mantiene contrato de operación de centro alterno en caso de daño permanente que imposibilite y restrinja la operación regular del centro de datos. La AR opera desde la oficina administrativa de Proveedor de Certificados PROCERT, C.A. que está localizada en un sitio distinto a los centros de datos y en la ciudad de Caracas, República Bolivariana de Venezuela.

5.1.2. Acceso físico.

Proveedor de Certificados PROCERT, C.A. dentro de su RPKI mantiene medidas de control de acceso tanto lógicas (aplicativo de certificación) como físicas (equipos) garantizando la integridad y seguridad de los servicios prestados. El acceso está restringido para personas que no sean operadores debidamente autorizados de la RPKI Proveedor de Certificados PROCERT, C.A. ha implantado un sistema de control de acceso físico que posee siete (7) capas de seguridad, desde el exterior hasta los servidores donde está instalada la CA de Proveedor de Certificados PROCERT, C.A. Además de procedimientos de seguridad que restringen el acceso solo a personal autorizado con autorización para el acceso a cada una de las siete (7) capas de seguridad física y requerir de información de acceso (usuario y clave) del sistema operativo de los equipos que conforman la CA de Proveedor de Certificados PROCERT, C. A. y los mecanismos físicos de seguridad para el manejo de la CA. El acceso físico para el interior del rack (apertura) debe estar permitido solo al personal del PSC PROCERT.

5.1.2. Electricidad y aire acondicionado.

Los centros de datos donde opera Proveedor de Certificados PROCERT, C. A. y su sede administrativa donde opera la AR cuentan con facilidades de servicio. Los centros de datos poseen alta redundancia a los fines de garantizar su continuidad operativa, y la gestión de la AR permite una operación remota en caso de estar comprometida la oficina administrativa de Proveedor de Certificados PROCERT, C. A.

5.1.3. Exposición al agua.

Los centros de datos donde opera Proveedor de Certificados PROCERT, C. A. cuentan con personal de soporte a los fines de prevenir cualquier falla o evento que afecte la operación de la CA. La sede administrativa donde opera la AR cuenta con personal de atención de incidencias a los fines de atender cualquier evento. La información de la AR se encuentra localizada en ambiente seguro y controlado dentro de los centros de

datos. Si por alguna razón se compromete la operación de la AR desde la sede administrativa la AR podrá operar de forma remota vía web.

5.1.4. Prevención y protección contra incendios.
Los centros de datos donde opera Proveedor de Certificados PROCERT, C. A. cuentan mecanismos de seguridad, prevención y combate de incendios a los fines de prevenir cualquier falla o evento que afecte la operación de la CA y garantizar la continuidad operativa. La sede administrativa donde opera la AR cuenta mecanismos de prevención, detección y combate de incendios que se mantiene regularmente a los fines de atender cualquier evento. La información de la AR se encuentra localizada en ambiente seguro y controlado dentro de los centros de datos. Si por alguna razón se compromete la operación de la AR desde la sede administrativa la AR podrá operar de forma remota vía web.

5.1.5. Almacenamiento de medios.
Los centros de datos donde opera Proveedor de Certificados PROCERT, C. A. cuentan mecanismos de seguridad, prevención y combate de incendios a los fines de prevenir cualquier falla o evento que afecte la operación de la CA y garantizar la continuidad operativa. La sede administrativa donde opera la AR cuenta mecanismos de prevención, detección y combate de incendios que se mantiene regularmente a los fines de atender cualquier evento. La información de la AR se encuentra localizada en ambiente seguro y controlado dentro de los centros de datos. Si por alguna razón se compromete la operación de la AR desde la sede administrativa la AR podrá operar de forma remota vía web.

5.1.6. Eliminación de residuos.
Proveedor de Certificados PROCERT, C. A. ha establecido procesos y procedimientos para la desincorporación de hardware y software, documentación e información de forma segura. Mantiene un esquema de clasificación de activos físicos e intangibles para manejar de forma adecuada su proceso de desincorporación sin afectar de ninguna manera la continuidad operativa de la RPKI de Proveedor de Certificados PROCERT, C. A.

5.1.7. Copia de seguridad externa.
Proveedor de Certificados PROCERT, C. A. mantiene un esquema de manejo y respaldo de la información a los fines de poder garantizar en todo momento la continuidad operativa y la recuperación ante cualquier desastre que pueda comprometer la operación de la RPPKI de Proveedor de Certificados PROCERT, C. A. Las copias de seguridad se almacenan de forma segura en sistemas especialmente diseñados para ellos a los fines de poder contar en todo momento y en caso de ser requerido con el acceso y manejo de los datos respaldados. El manejo de las claves de acceso a dicha información se maneja de forma segura y a los fines de prevenir fugas de datos o extracción de datos por parte de personal no autorizado de Proveedor de Certificados PROCERT, C. A.

5.2. Controles de procedimiento.

Proveedor de Certificados PROCERT, C. A. procede a establecer los procedimientos, controles y recursos que maneja a los fines de mantener su RPKI y poder emitir de manera conforme certificados electrónicos para los Signatarios o entidades finales usuarias de certificado electrónico.

5.2.1. Roles de confianza.

Proveedor de Certificados PROCERT, C. A. mantiene un esquema interno operacional que establece roles y funciones dentro de la RPKI, asignando determinadas actividades y reservando a personal de confianza la ejecución de funciones que requieren alta capacitación y confianza y que aplica a las actividades de mantenimiento y operación de la CA y RA de Proveedor de Certificados PROCERT, C. A. Todo el personal mantiene obligaciones contractuales de confidencialidad de la información y descripciones de cargo que establecen y delimitan sus responsabilidades. Se requiere una capacitación previa para la permanencia dentro de la RPKI de Proveedor de Certificados PROCERT, C. A. y se establecen mecanismos regulares de prueba y revisión del cumplimiento de roles y funciones, los cuales están segregados y establecidos de tal manera que requieren la operación concurrente que involucra al personal y la alta dirección de Proveedor de Certificados PROCERT, C. A. en la operación y manejo de la CA y RA de Proveedor de Certificados PROCERT, C. A.

5.2.2. Número de personas necesarias por tarea.

Proveedor de Certificados PROCERT, C. A. mantiene un esquema interno operacional que establece roles y funciones dentro de la RPKI, los cuales están segregados y establecidos de tal manera que requieren la operación concurrente que involucra al personal y la alta dirección de Proveedor de Certificados PROCERT, C. A. en la operación y manejo de la CA y RA de Proveedor de Certificados PROCERT, C. A. Para la administración de la CA existen dos administradores que validan y autorizan la emisión de las claves, para la operación de la AR existen dos administradores encargados de validar la identidad de los Signatarios o entidades finales usuarias de certificados electrónicos, para la operación regular de la CA existen un cuerpo de operadores debidamente calificados para la tarea y un auditor encargado de verificar el cumplimiento de los procedimientos y métodos internos dentro de Proveedor de Certificados PROCERT, C. A.

5.2.3. Identificación y autenticación de cada rol.

Proveedor de Certificados PROCERT, C. A. mantiene un esquema interno de seguridad con políticas que contemplan la revisión periódica de los mecanismos de autenticación, a los fines de su actualización y mejora recurrente de claves de acceso lógico. Todo acceso a la CA, RA y los sistemas administrativos y de gestión de Proveedor de Certificados PROCERT, C. A., es controlado y verificado con mecanismos de comprobación seguros que incluyen biometría, códigos temporales y claves robustas de acceso, todo en función del nivel de criticidad y confidencialidad de la información.

5.2.4. Funciones que requieren separación de funciones.

Proveedor de Certificados PROCERT, C. A. posee una política interna de segregación de roles, funciones y descripciones de cargo dentro de la AC y AR, lo cual permite establecer las diferenciaciones requeridas y necesarias para prevenir riesgos operacionales, de manejo de claves de los Signatarios o de la información suministrada por estos; todo ellos para prevenir que una persona asuma múltiples funciones dentro de la RPKI, lo cual se pueda traducir en riesgo y por ende pérdida de la confianza en Proveedor de Certificados PROCERT, C. A. Por descripción de cargo los encargados de la CA no pueden asumir otras funciones no indicadas en su descripción de cargo; al igual que los de la AR, el oficial de cumplimiento y el auditor de sistemas.

5.3. Controles de personal.

5.3.1. Cualificaciones, experiencia y requisitos de autorización.

Proveedor de Certificados PROCERT, C. A. posee una política de reclutamiento y selección de personal que establece el proceso de ingreso de personal calificado para cada tarea de la CA y la AR. Una vez ingresado el personal, se aplica la política de adiestramiento y capacitación del personal, a los fines de garantizar que todo nuevo ingreso conozca la operación de la CA o AR que le ha sido asignada. Solo después de superar de forma satisfactoria y comprobada las evaluaciones de sus capacidades funcionales, es cuando se le asigna un rol dentro de la CA y AR de Proveedor de Certificados PROCERT, C. A. Al proceder de esta manera Proveedor de Certificados PROCERT, C. A. asegura que su personal maneje de forma esperada las funciones, roles y competencias profesionales asignadas a su cargo, aumentando el nivel de confianza de los Signatarios. Se mantiene un esquema de supervisión activa y existen mecanismos automatizados como el SOC y NOC que permiten establecer de forma inmediata la ocurrencia de un evento derivado de alguna inobservancia o incumplimiento de los roles y funciones de los trabajadores de la RPKI de Proveedor de Certificados PROCERT, C. A.

5.3.2. Procedimientos de verificación de antecedentes.

Proveedor de Certificados PROCERT, C. A. posee una política de reclutamiento y selección de personal que establece el proceso de verificación de identidad de los candidatos, validación de documentos de identidad, referencias personales y el cumplimiento de la política conoce a tu empleado. Dentro de la República Bolivariana es inconstitucional hacer la revisión de antecedentes criminales a los fines de la selección laboral.

5.3.3. Requisitos de formación.

Proveedor de Certificados PROCERT, C. A. posee una política de reclutamiento y selección de personal, junto a una política de descripción de puesto de trabajo, las cuales permiten efectuar una validación preliminar de las competencias y capacidades del personal que será contratado. Adicionalmente, de forma periódica se ejecutan labores internas de capacitación del personal en las labores a las cuales son asignados dentro de la operación regular de la CA y AR de Proveedor de Certificados PROCERT, C. A. y a los fines de garantizar una respuesta esperada en caso de recuperación ante desastres, validación conforme de los Signatarios y la

gestión segura de las claves. Dentro de las fortalezas y capacitaciones otorgadas al personal de Proveedor de Certificados PROCERT, C. A. se encuentran el manejo de conocimientos básico, intermedios y avanzados de operación de RPKI, seguridad de información, recuperación ante desastres, cumplimiento de los lineamientos del CA Browser Fórum, normas internacionales y legislación de la República Bolivariana de Venezuela, procedimientos de verificación de documentación y validación de entidades y personas a los fines de cumplir los requisitos de la AR.

5.3.4. Frecuencia y requisitos de reentrenamiento.
Proveedor de Certificados PROCERT, C. A. posee una política de adiestramiento y desarrollo de personal que contempla la planificación de las competencias requeridas por los distintos cargos dentro de la RPKI para desempeñar sus cargos en cumplimiento de los mejores prácticas y estándares nacionales e internacionales en materia de operación de RPKI, seguridad de información, recuperación ante desastres, cumplimiento de los lineamientos del CA Browser Fórum, normas internacionales y legislación de la República Bolivariana de Venezuela, procedimientos de verificación de documentación y validación de entidades y personas a los fines de cumplir los requisitos de la AR.

5.3.5. Frecuencia y secuencia de rotación de puestos.
No se contemplan rotación de puestos, existe una descripción de puesto asociado a cada cargo.

5.3.6. Sanciones por acciones no autorizadas.
Proveedor de Certificados PROCERT, C. A. en sus contratos de trabajo y en los documentos de políticas internas, establecen las medidas correctivas por incumplimiento u omisión de las obligaciones que impone la relación laboral con Proveedor de Certificados PROCERT, C. A.; fijando las medidas preventivas y sancionatorias que contemplan desincorporación del puesto de trabajo y la ejecución de medidas que pueden ser de índole administrativa, civil y/o penal. Iguales previsiones aplican para los prestadores de servicio y proveedores que incumplan las políticas de Proveedor de Certificados PROCERT, C. A.

5.3.7. Requisitos del contratista independiente.
Proveedor de Certificados PROCERT, C. A. posee una política de selección y contratación de proveedores de bienes y servicios que establece que en las áreas que involucren las contrataciones de bienes y servicios para la RPKI, los bienes o los servicios deben cumplir con el estándar internacional establecido por el CA Browser Fórum, las normas dictadas por la SUSCERTE y la legislación que regula la materia dentro de la República Bolivariana de Venezuela. El modelo de contrato de Proveedor de Certificados PROCERT, C. A. contempla una cláusula que establece la previsión de declaración de contratista independiente y una de confidencialidad de la información. Igualmente establece dicho contrato que el incumpliendo de las normas y reglas contractuales de Proveedor de Certificados PROCERT, C. A., puede acarrear la imposición de sanciones de índole administrativa, civil y/o penal.

5.3.8. Documentación facilitada al personal.

Proveedor de Certificados PROCERT, C. A. posee una política de Roles y funciones y de seguridad de la Información que establecen que el personal de la RPKI que contempla a los operadores de la CA y de la AR, solo contarán con el acceso a la información y documentación requerida para el desempeño de su cargo y la descripción de puesto establecida por Proveedor de Certificados PROCERT, C. A. y a los fines de garantizar el cumplimiento del estándar internacional establecido por el CA Browser Fórum, las normas dictadas por la SUSCERTE y la legislación que regula la materia dentro de la República Bolivariana de Venezuela. Los incumplimientos por parte del personal de Proveedor de Certificados PROCERT, C. A. puede generar la aplicación de medidas sancionatorias que pueden ser de índole administrativa, civil, laboral y/o penal.

5.4. Procedimientos de registro de auditoría.

Proveedor de Certificados PROCERT, C. A., configura y mantiene un registro de los eventos de auditoría de la plataforma RPKI, estableciendo un esquema de respaldo y protección de los logs de auditoría de la RPKI, los cuales incluyen la CA y la AR. Los registros de auditoría electrónicos de eventos (logs) son registros que permiten establecer la trazabilidad de las actividades y operaciones ejecutadas dentro de la plataforma RPKI de Proveedor de Certificados PROCERT, C. A. Estos registros son almacenados de forma automática y electrónica.

5.4.1. Tipos de eventos registrados.

Los registros de auditoría electrónicos de eventos (logs) que deben ser mantenidos por cada una de las SubCA de Proveedor de Certificados PROCERT, C. A., incluyen los siguientes eventos o actividades de la RPKI:

- Eventos de los equipos que conforman la plataforma de la CA:
  - Instalación y configuración del sistema operativo.
  - Instalación y configuración de cualquier aplicación instalada en el equipo.
  - Instalación y configuración de la autoridad de certificación.
  - Instalación y configuración del módulo criptográfico.
  - Accesos o intentos de acceso al equipo.
  - Actualizaciones.
  - Realización de copias de seguridad
  - Generación y gestión de la LCR.
  - Mantenimiento y funcionamiento del OCSP.
  - Generación de certificados.
  - Manejo de ciclo de vida de los certificados.
  - Manejo de plantillas de certificados y cambios en las mismas.
  - Eventos del software de certificación:
    - Gestión de usuarios.
    - Gestión de roles.
    - Gestión de plantillas de certificados.
    - Lista de control de acceso (ACLs).
    - Gestión de certificados (todo lo contemplado en el ciclo su vida)
  - Eventos relacionados con el acceso físico:
    - Acceso del personal al centro de datos.

- Acceso del personal a los equipos y sistemas.
- Eventos de acciones correctivas:
  - Errores de hardware.
  - Errores de software.

Cada registro de eventos incluye datos relativos a la fecha y hora en que se produjo, número de serie, descripción del evento y el sistema o persona que lo origino.

5.4.2. Registro de frecuencia de tratamiento.

Los registros de auditoría electrónicos de eventos (logs) se llevan a cabo en cualquier momento que se realice una operación dentro de la RPKI de Proveedor de Certificados PROCERT, C. A., lo cual incluye la CA y la AR. El personal de operaciones notifica a su administrador de seguridad cuando un proceso o acción causa un evento crítico de seguridad o discrepancia siguiendo la política interna de Proveedor de Certificados PROCERT, C. A., respecto al manejo del SOC, NOC y el plan integral de riesgos y seguridad de la información de Proveedor de Certificados PROCERT, C. A.

Los registros de auditoría electrónicos de eventos (logs) se mantienen en su SubCA de Proveedor de Certificados PROCERT, C. A. La revisión de los registros de auditoría electrónicos de eventos (logs) es notificada por el personal de operaciones que detecta la situación en el SOC, NOC o de los registros generados por la plataforma RPKI, escalando el caso a sus supervisores, a los fines de activar los mecanismos necesarios en caso de un evento de seguridad o falla en cualquiera de los componentes de la RPKI. En todo caso, se debe cumplir el proceso de registro de evento y control operacional correspondiente que involucra el Comité de Seguridad de la información, el cual establecerá los pasos que se deberán seguir.

5.4.3. Período de retención para el registro de auditoría.

Los registros de auditoría electrónicos de eventos (logs) se retienen por un período de diez (10) años.

5.4.4. Protección del registro de auditoría.

Los registros de auditoría electrónicos de eventos (logs) son centralizados por un servicio que los colecta y firma electrónicamente a los fines de garantizar su integridad y prevenir su manipulación. El sistema es mantenido mediante mecanismos de control de acceso y separación de roles con relación al software y el hardware que manejan la recolección automática y mediante procedimientos operacionales confidencialmente documentados, conocidos y seguidos por el personal de Proveedor de Certificados PROCERT, C. A.

5.4.4. Protección del registro de auditoría.

Los registros de auditoría electrónicos de eventos (logs) son centralizados y se extraen de forma automatizada del equipo, segregando el equipo o servicio desde donde se generan; siendo firmados electrónicamente para prevenir su manipulación o alteración. Los registros de auditoría electrónicos de eventos (logs) son almacenados de forma segura y le es

aplicable una política de control de acceso que restringe y previene permisos accesos no autorizados, modificación, sustitución o destrucción. Para los logs del servicio de estampado de tiempo se coloca a disposición de los usuarios el registro de log que muestran las asignaciones de token de tiempo a los fines de que sea expedito y sencillo el proceso de validación del servicio.

5.4.5. Procedimientos de copia de seguridad del registro de auditoría.
Estos registros de auditoría electrónicos de eventos (logs) permite auditar y verificar los intentos de accesos, los accesos y las operaciones dañinas, sean estas intencionales o no. Los registros de auditoría electrónicos de eventos (logs) son almacenados igualmente en un respaldo en nube en un sitio seguro distinto del centro de datos principal. Los respaldos de los registros de auditoría electrónicos de eventos (logs), se programan respaldos periódicos para cosos de seguridad bajo un esquema incremental diario, semanal y mensual, que permita contar con la información requerida para el caso de un evento de recuperación ante desastres.

5.4.6. Sistema de Recolección de Auditorías (Interno vs. Externo).
Los registros de auditoría electrónicos de eventos (logs) son centralizados por un servicio de Proveedor de Certificados PROCERT, C. A. que los colecta y firma electrónicamente a los fines de garantizar su integridad y prevenir su manipulación; la colecta de los logs es automatizada y desde el inicio de funcionamiento de los equipos o servicios; dichos registros son almacenamos de forma segura y confidencial. Existe un sistema de monitoreo del funcionamiento del sistema de los registros de auditoría electrónicos de eventos (logs), el cual envía mensajes de alerta al SOC, respecto a fallas en el funcionamiento del sistema de registro de Logs, activando las actividades de remediación orientadas al restablecimiento de dicho servicio y el registro debido de todos los logs de la RPKI.

5.4.7. Notificación al sujeto causante del evento [OMITIDO].
Bajo la legislación vigente dentro de la República Bolivariana de Venezuela, todo sujeto que por acción u omisión cause un daño o afecte un sistema informático será responsable del hecho. Proveedor de Certificados PROCERT, C. A. se reserva la acción en contra de cualquier Signatario o empleado o contratista de Proveedor de Certificados PROCERT, C. A. que mediante registro de Logs quede evidenciada su responsabilidad o acción de daño o sabotaje de cualquier naturaleza contra la RPKI de Proveedor de Certificados PROCERT, C. A.

5.4.8. Evaluaciones de vulnerabilidad.
Proveedor de Certificados PROCERT, C. A., a los fines de dar cumplimento a las previsiones del CAB Browser Fórum, del Webtrust y de la SUSCERTE, mantiene un esquema anual de auditoría de cumplimiento de los requisitos impuestos para aplicar a la certificación como entidad reconocida y proveedor de servicios de certificación dentro de la República Bolivariana de Venezuela. En adición a lo anterior y de conformidad con la Política de Seguridad de la Información de Proveedor de Certificados PROCERT, C. A., se ejecutan auditorías de cumplimiento periódicas a los fines de comprobar y verificar el pleno cumplimiento por parte del

personal directivos y contratistas de Proveedor de Certificados PROCERT, C. A., de todas las normas de seguridad de la información confidencialidad y mantenimiento de PKI aplicables a una CA. Dentro de las actividades contempladas de evalúa la seguridad de los sistemas, la integridad del proceso de generación de certificados, análisis de vulnerabilidades de la RPKI; dichos análisis son ejecutados por personal de confianza debidamente capacitado y autorizado para ello.

5.5. Archivo de registros [OMITIDO].

Proveedor de Certificados PROCERT, C. A., dentro de su política de seguridad de información y plan de plan integral de riesgos y seguridad de la información, contempla la ejecución de registros de auditoría electrónicos de eventos (logs), su resguardo, protección y almacenamiento en centro principal y alterno, administración y manejo por parte del personal de Proveedor de Certificados PROCERT, C. A. El resguardo de los registros de auditoría electrónicos de eventos (logs), se orienta al cumplimiento de las mejoras prácticas internacionales las previsiones del CAB Browser Fórum, del Webtrust y de la SUSCERTE. Los registros que mantiene Proveedor de Certificados PROCERT, C. A. se indican en el aparte 5.4.1. (Tipos de eventos registrados) de esta CPS y el período de retención de diez (10) años.

5.6. Cambio de clave.

Proveedor de Certificados PROCERT, C. A., contempla que los procesos de cambio de clave que involucren la SubCA de S/MIME, serán ejecutadas en cumplimiento de las mejores prácticas internacionales las previsiones del CAB Browser Fórum, del Webtrust y de la SUSCERTE. Las nuevas claves serán generadas y resguardadas de forma segura y se procederá a la publicación de los enlaces correspondientes de comprobación correspondientes a la LCR y OCSP de dichas nuevas claves. Las claves que sean sustituidas por cambio de algoritmo se mantendrán vigente hasta tanto se proceda a la reemisión d ellos certificados generados bajo el algoritmo sustituido. En el caso del vencimiento de la vigencia del certificado de la SubCA que corresponda, se procederá a la emisión del nuevo par de claves por el período de tiempo que se ajuste el período contratado por el Signatario o entidad final usuario de certificados electrónicos emitidos por la RPKI de Proveedor de Certificados PROCERT, C. A.

5.7. Compromiso y recuperación ante desastres.

Proveedor de Certificados PROCERT, C. A., ha implantado un plan de continuidad de negocio y recuperación ante desastres. Bajo un escenario que establezca un eventual compromiso parcial o total de la RPKI que afecte la CA o la AR. El plan de recuperación ante desastre es revisado cada seis meses a la luz de los cambios riesgos en el ambiente y a los fines de mantenerlo actualizado. El plan de recuperación ante desastre contempla los siguientes puntos:

- Fallas/corrupción de recursos de computación;
- Compromiso de la Integridad de la clave; y
- Desastres naturales y terminación.

En el plan de continuidad de negocio y recuperación ante desastre (PRD), se especifica el procedimiento a realizar en cada uno de los escenarios considerados como desastre y es ejecutado por el personal de Proveedor de Certificados

PROCERT, C. A. El compromiso total o parcial de la RPKI se notifica a los Signatarios, entidades finales usuarias de certificados electrónicos y la SUSCERTE. El personal de Proveedor de Certificados PROCERT, C. A., debe tomar los correctivos y emprender las actividades necesarias para restablecer la RPKI en el momento de presentarse un escenario de desastre a los fines de restablecer en el más corto plazo su operación y mantener la confianza en el RPKI.

5.7.1. Alteración de los recursos, hardware, software y/o datos.
Proveedor de Certificados PROCERT, C. A., contempla la revisión periódica de sus sistemas, softwares y demás elementos que constituyen su plataforma de RPKI, si de las revisiones y evaluaciones periódicas se determina el compromiso de uno o varios de los recursos informáticos; se procederá de inmediato a declarar el compromiso parcial o total y revocará los certificados que estén involucrados o los servicios de Proveedor de Certificados PROCERT, C. A., que estén afectados, notificando debidamente a los Signatarios o las entidades finales usuarias de certificados electrónicos. Subsanados los puntos que generaron la afectación parcial o total y debidamente restablecida la RPKI, se proporcionaran nuevas claves a los Signatarios y se continuara prestando los servicios que hayan sido interrumpidos.

5.7.2. Procedimiento de actuación ante la vulnerabilidad de la clave privada de una autoridad.
Proveedor de Certificados PROCERT, C. A., declara que en la eventualidad del compromiso de su clave privad de una de sus SubCA, que sea detectado, evaluado y establecido por el personal de Proveedor de Certificados PROCERT, C. A, se procederá de la siguiente manera:

- Declaración del escenario de desastre.
- Notificación a la SUSCERTE del compromiso de la clave, para la inmediata revocación del certificado de Proveedor de Certificados PROCERT, C. A.
- Publicación del evento en la Página Web de Proveedor de Certificados PROCERT, C. A.
- Notificación a los Signatarios.
- Notificar a la compañía aseguradora que mantiene la fianza de operación de Proveedor de Certificados PROCERT, C. A.
- Analizar el motivo del compromiso y realizar un informe técnico detallando las razones por las que se vio comprometida la clave privada de Proveedor de Certificados PROCERT, C. A.
- Acordar junto con la SUSCERTE las acciones a tomar para la reactivación del servicio de emisión de certificados.

5.7.3. Seguridad de las instalaciones tras un desastre natural o de otro tipo.
Proveedor de Certificados PROCERT, C. A., ha implantado un plan de continuidad de negocio y recuperación ante desastres. Bajo dicho plan se mantienen dos facilidades de centros de datos que se encuentran suficientemente diferenciadas y separadas territorial y geográficamente a los fines de poder garantizar que ante de un evento catastrófico o desastre que comprometa la operación de un centro de datos, se cuente con uno

alterno para poder seguir prestando los servicios de RPKI. Proveedor de Certificados PROCERT, C. A.

5.8. Rescisión de CA o RA.

Proveedor de Certificados PROCERT, C. A., tiene contemplado que los supuestos para que ocurra una cesación de operaciones son los siguientes supuestos:

- Extinción por vencimiento de acreditación.
- Extinción por cese de operaciones.
- Extinción por revocación de acreditación. En este caso, y solo por razones comprobadas de incumplimiento, procederá la ejecución de la garantía solicitada por la SUSCERTE al momento de la acreditación
- Extinción derivada de aspectos tecnológicos.

En el caso de ocurrencia de cualquier de los supuestos antes indicados Proveedor de Certificados PROCERT, C. A., estará en la obligación de colocar a disposición de la SUSCERTE el repositorio de todos los certificados emitidos durante su gestión, incluyendo el estatus de cada uno de ellos. Proveedor de Certificados PROCERT, C. A., igualmente procederá con los Signatarios de la siguiente manera:

- Notificar el cese y fecha de terminación a los Signatarios por correo electrónico, con treinta días de antelación a la fecha de terminación.
- Informar a los Signatarios que entidad asume la operación o la RPKI.
- En caso de no asumir ninguna entidad la PKI suministrar el acceso a la SUSCERTE para mantener activos los publicadores de la LCR y OCSP hasta el vencimiento de los certificados que hayan sido emitidos por Proveedor de Certificados PROCERT, C. A.

6. Controles técnicos de seguridad.

En esta sección se describen los controles de seguridad utilizados por Proveedor de Certificados PROCERT, C. A., para la gestión, manejo y generación de claves criptográficas.

6.1. Generación e instalación de pares de claves.

6.1.1. Generación de pares de claves.

Proveedor de Certificados PROCERT, C. A., genera el par de claves (pública y privada) de su SubCA S/MIME utilizando un dispositivo de hardware criptográfico (HSM) que cumple con el FIPS 140-2 Nivel 3. La generación del par de claves de cada SubCA de Proveedor de Certificados PROCERT, C. A., se encuentra configuradas para que sean segregadas en varias personas de confianza dentro de Proveedor de Certificados PROCERT, C. A. y siguiendo el estándar internacional de seguridad en la operación de la CA. Es requerida la participación concurrente de las personas que administran la CA para efectuar operaciones dentro de la CA que superen la simple administración. Todas las funciones y roles se encuentran descritos en el documento del Manual y Modelo de Operación de la CA. La generación del par de claves de las SubCA de Proveedor de Certificados PROCERT, C. A., se ejecutan en cumplimiento de las presiones del CA Browser Fórum y las normas impuestas por la SUSCERTE.

La CA está configurada de tal manera de dejar registro en Logs de las personas y actividades que han interactuado o se han ejecutados dentro de la CA.

Los Signatarios de la SubCA S/MIME deben generar en línea su par de claves criptográficas a los fines de que sea tramitada y aprobada su solicitud de certificado. Proveedor de Certificados PROCERT, C. A., no genera el par de claves del Signatario. Las peticiones generadas por los Signatarios se hacen a través del Sistema AR, debiendo ingresar sus usuarios y claves para acceder, luego debe el Signatario cargar toda su información y ser validado por la AR; una vez validado por la AR, el operador AR aprueba dentro del Sistema AR. Una vez aprobado el Signatario por la AR el sistema le envía un mensaje para que acceda al Sistema AR y genere su petición de certificado a través del Sistema AR. Generada la petición, la misma es notificada por correo a la AR y al operador de la CA, para que proceda a la aprobación de la petición del Signatario contra el dispositivo HSM, quedando debidamente almacenada. Una vez aprobadas el par de claves, el Signatario deberá ingresar con su usuario y clave dentro del Sistema AR y seleccionar descarga del certificado; seguidamente el sistema enviará un OTP al teléfono del usuario y este deberá colocar el pin de seguridad para poder acceder a la descarga del certificado. Para la descarga el sistema exigirá que el usuario coloque una clave de seguridad para acceder a su certificado. En los certificados S/MIME generados por la CA de Proveedor de Certificados PROCERT, C. A., el valor id-kp-emailProtection debe estar presente y los valores id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage no deben estar presentes.

En virtud de lo anterior, si el cliente extravía su clave privada, se deberá proceder a la emisión de un nuevo certificado y deberá cumplir nuevamente el proceso de contratación de Proveedor de Certificados PROCERT, C. A. La clave pública siempre estará en el repositorio, de conformidad con lo establecido en la presente CPS.

6.1.2. Entrega de clave privada al suscriptor.

El proceso de entrega del par de claves generadas por la CA de Proveedor de Certificados PROCERT, C. A., en la SubCA S/MIME se describe a continuación y a los fines que el Signatario tome las precauciones necesarias a fin de garantizar la protección de la clave privada:

- El usuario final debe ingresar a la página web de Proveedor de Certificados PROCERT, C. A., (http://www.procert.net.ve) presionar clic sobre el botón de SISTEMA AR (procert.net.ve/sistemaAR/login.aspx) y de esta forma ingresar al servicio web.

- Allí debe de verificar que los datos contenidos están correctos**,** dicha solicitud está compuesta en cuatro (04) partes:

    - Información del Usuario: Esta sección contiene el nombre y apellido del usuario que fue suministrado a Proveedor de Certificados PROCERT, C. A.

- Subject: Información general del usuario que, dependiendo del tipo de certificado, algunos campos serán obligatorios, a continuación, se enlista los campos y cuales son obligatorios por certificados
- Información del nombre alternativo: En esta sección debe de contener el número de RIF o C.I. del signatario
- Opciones de clave: En esta sección se debe escoger el Proveedor de Servicios Criptográfico (CSP), Posteriormente el usuario debe aceptar los términos y condiciones para habilitar el botón generar. Luego de presionar el botón generar el usuario tendrá la opción de proteger su clave privada con un nivel de seguridad alto utilizando una contraseña.

- Seguidamente, la AR revisa y evalúa la solicitud del Signatario y en caso de estar conforme procede a la aprobación de esta. Una vez aprobada la solicitud del Signatario pasa a la aprobación de la CA y es cuando el botón de generación de par de claves se activa para el operador de la CA, quien contra el HSM procede a la aprobación de la petición del Signatario.

- Posterior a la aprobación de la solicitud por la CA, se enviará al correo del usuario un enlace, a través del cual i accediendo el Signatario podrá descargar el certificado. El procedimiento de generación de par de claves mencionado garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, Proveedor de Certificados PROCERT, C. A., solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

6.1.3. Entrega de clave pública al emisor del certificado.
La CA de Proveedor de Certificados PROCERT, C. A., al momento de recibir el CSR generado por el Signatario, procede a la firma y generación del par de claves criptográficas que forman el certificado. La clave publica se mantiene dentro del certificado y es almacenada de forma automatizada por la CA en su repositorio de certificados emitidos.

6.1.4. Entrega de claves públicas de CA a usuarios de confianza.
Proveedor de Certificados PROCERT, C. A., se encuentra en la obligación de mantener en su repositorio y disponible su clave pública, la cual cualquier cliente o parte interesada puede acceder a través de la página Web de PROCERT (https://www.procert.net.ve/ConsultaPublica/index.aspx).

6.1.5. Tamaños de las claves.
Los módulos de la raíz de certificación de la autoridad de certificación (AC) y las claves tienen una longitud de al menos 4096 bits y utilizan el algoritmo RSA y de al menos 256 bits en el caso del algoritmo de curva elíptica ECC (ECDSA).

6.1.6. Generación de parámetros de clave pública y control de calidad.
Los parámetros utilizados para la generación de las claves públicas cumplen con los requerimientos FIPS 140-2 Nivel 3. La generación del par de claves (pública y privada) que utiliza la plataforma de certificación de Proveedor de Certificados PROCERT, C. A., es un proceso sencillo, pero que

requiere de precauciones especiales y son generados con un equipo HSM.

6.1.7. Propósitos de uso de claves (según el campo de uso de claves X.509 v3).

Proveedor de Certificados PROCERT, C. A., genera sus certificados electrónicos bajo estándar internacional X.509v3 e incluyen campos de extensión de uso de claves que especifican el uso previsto del certificado electrónico conforme a lo establecido en la CP. Usos distintos a los declarados en la CP no son permitidos. Adicionalmente y al ser subordinada a la Raíz de Certificación del Estado Venezolano, Proveedor de Certificados PROCERT, C. A., se contemplan la emisión de certificados para Signatarios usuarios de certificados electrónicos a través de una SubCA identificada como S/MIME. A continuación, se procede a indicar las limitaciones aplicadas a los certificados generados por las SubCA antes indicadas y que son las siguientes:

- Limitaciones de emisión para certificados end entity del tipo S/MIME:
  - El valor id-kp-emailProtection debe estar presente.
  - Los valores id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage no deben estar presentes.

El uso de clase de la SubCA de Proveedor de Certificados PROCERT, C. A., varía en función del uso asignado al certificado y que está contemplado y se describe de forma detallada en la CP. A continuación, se enuncian los usos asignados a las claves de las SubCA de Proveedor de Certificados PROCERT, C. A.:

- Firma de Certificados a las SubCA de S/MIME.
- Firma de certificados establecidos en la CP.
- Firma del certificado requerido para el servicio OSCP
- Firma de la lista de certificados revocados.
- Firma de certificados requeridos para la operación de la RPKI y otros servicios de Proveedor de Certificados PROCERT, C. A.

6.2. Protección de claves privadas e ingeniería de módulos criptográficos.

6.2.1. Estándares y controles de módulos criptográficos.

El módulo criptográfico usado por la RPKI de Proveedor de Certificados PROCERT, C. A., está certificado para cumplir con los requerimientos de FIPS 140-2 nivel 3, Common Criteria EAL 4+ o equivalente. En el caso de la raíz de certificación de PROCERT, dicho modulo se mantiene fuera de línea.

6.2.2. Clave privada (n de m) Control multipersona.

Las Claves privadas de las SubCA de Proveedor de Certificados PROCERT, C. A., se encuentra bajo control multipersona. Estas se activan mediante la inicialización del software de la CA por medio de una combinación de operadores de la CA, Administradores del HSM y usuarios del sistema operativo. Este es el único método de activación de dichas claves. Los mecanismos de acceso y control se ejecutan a través de token o

tarjetas inteligentes y claves diferenciadas y asociadas a determinados roles dentro de la administración de la CA de la RPKI

6.2.3. Custodia de clave privada.

La clave privada de la CA de Proveedor de Certificados PROCERT, C. A. está protegida por un HSM. La CA ha establecido los pasos a seguir para la instalación del HSM, los mismos se detallan a continuación:

- Instalación de los drivers: Se deberá instalar los drivers correspondientes al HSM en el servidor de CA.
- Instalación física.
- Creación del Mundo de Seguridad.
- Se crean y asignan los perfiles y roles dentro del mundo de seguridad.
- Se configuran con los tokens y tarjetas los distintos roles dentro de la CA y la RPKI.

6.2.4. Copia de seguridad de clave privada.

Las copias de seguridad de las claves privadas de las SubCA que son generados en el HSM se almacenan de forma segura, en una bóveda externa al sitio de operación de la CA de Proveedor de Certificados PROCERT, C. A. y requieren de un acceso controlada los fines de poder disponer de dichas copias. Para la restauración del mundo de seguridad de las SubCA, es necesaria la participación concurrente de personas de confianza de Proveedor de Certificados PROCERT, C. A., sin lo cual las copias de seguridad no podrán ser usadas. Los Signatarios de la SubCA S/MIME genera sus propias claves privadas que son gestionadas a través de la CA pero que son almacenadas en los repositorios de los Signatarios.

6.2.5. Archivo de clave privada.

Proveedor de Certificados PROCERT, C. A., establece que al expirar la videncia de los certificados de la SubCA S/MIME, se procede al archivo en bóveda por un período de diez (10) años conforme a las obligaciones impuestas por la SUSCERTE.

6.2.6. Transferencia de clave privada hacia o desde un módulo criptográfico.

Proveedor de Certificados PROCERT, C. A., establece como regla que todas las claves deben ser generadas a través de un HSM que debe contar con la debida configuración de roles y segmentación de funciones a los fines de establecer un esquema multipersona de autorizaciones, A los fines de su respaldo las claves privadas pueden ser exportadas y se procede a su cifrado para almacenarlas en un dispositivo seguro en bóveda ubicada en un lugar distinto al sitio de operación de la RPKI pero accesible en caso de activar un proceso de recuperación ate desastres. El compromiso de la clave privada genera su inmediata revocación y activación d ellos protocoles de recuperación ante desastres.

6.2.7. Almacenamiento de claves privadas en el módulo criptográfico.

Proveedor de Certificados PROCERT, C. A., ha establecido los parámetros y lineamientos bajo los cuales se hará la generación de las claves de la SubCA de S/MIME a los fines de garantizar la integridad de estas y

cumplir con los lineamientos del CA Browser Fórum y la SUSCERTE. A continuación, se detallan dichos lineamientos y parámetros:

- Se generará un mundo de seguridad por cada SubCA.
- Se instalará la autoridad de certificación bajo la modalidad de Subordinada y se generará la petición de certificado para cada SubCA desde el HSM.
- La SUSCERTE firmará la solicitud del certificado de cada SubCA.
- Se instalará y activará el certificado de cada SubCA en el HSM.

El HSM de Proveedor de Certificados PROCERT, C. A., cumple el estándar FIPS 140-2 Nivel 3. Todas las claves privadas raíz de las SubCA de Proveedor de Certificados PROCERT, C. A., se almacenan fuera de línea.

6.2.8. Método de activación de la clave privada.

Para la activación de las claves privadas es necesario utilizar la distribución de tokens de seguridad que se crearon al crear el mundo de seguridad y el manejo de la RPKI y las tarjetas inteligentes asignadas a cada uno de los roles, en la distribución de roles concurrentes o necesarios para cada actividad, adicionalmente, es necesario el acceso al sistema operativo del servidor de certificación y al centro de datos donde se encuentra operando la CA.

Los Signatarios de Proveedor de Certificados PROCERT, C. A., deben cumplir las instrucciones de uso y descarga del certificado electrónico, las cuales indican la obligación del Signatario de asignar una clave de uso para su certificado. Los Signatarios son los únicos responsables de resguardar la seguridad de su clave privada, cualquier compromiso de la esta, debe generar la revocación del certificado a través de la autogestión del Signatario por medio del Sistema AR o de la debida notificación del compromiso de clave a Proveedor de Certificados PROCERT, C. A., a través del correo soporte@procert.net.ve.

6.2.9. Método de desactivación de la clave privada.

El HSM de Proveedor de Certificados PROCERT, C. A., posee los atributos para que a través de comando asignados a roles compartidos de administración del HSM sea posible desactivar temporalmente las claves privadas de cada uno o todas las SubCA de Proveedor de Certificados PROCERT, C. A. No obstante, las SubCa de Proveedor de Certificados PROCERT, C. A., se mantienen activas pero administradas a través de una participación de tokens y tarjetas con roles de administración predefinidos y que requieren de actividad concurrente de personal de confianza. Los certificados finales de Signatarios no pueden ser suspendidos por estos; solo es posible suspender usuarios del Sistema AR mediante la intervención del personal de la AR y CA y por acción debidamente justificada y soportada. Los certificados solo aceptan la revocación como método de finalización o restricción de uso.

6.2.10. Método de destrucción de la clave privada.

El HSM de Proveedor de Certificados PROCERT, C. A., posee los atributos para que a través de comando asignados a roles compartidos de administración del HSM sea posible la revocación o destrucción de las claves privadas de cada una o todas las SubCA de Proveedor de Certificados PROCERT, C. A. Las claves privadas correspondientes a certificado que han cumplido su ciclo de vida o han sido revocados pueden ser borradas del repositorio seguro del HSM. Los certificados finales de Signatarios pueden ser revocados y borrada la clave privada del repositorio en donde se encuentren almacenada; esta acción la puede ejecutar directamente el Signatario a través del Sistema AR o mediante la intervención del personal de la AR y CA, por acción debidamente justificada y soportada. La eliminación de la clave privada de cada una de las SubCA contempla igualmente las que han sido respaldadas por temas de seguridad y continuidad de negocio, una vez se ha revocado o expirado el tiempo de vigencia del certificado que corresponda.

6.2.11. Clasificación del módulo criptográfico.

El HSM de Proveedor de Certificados PROCERT, C. A., es un dispositivo de hardware compuesto por un módulo criptográfico que es utilizado para almacenar de forma segura la clave privada de cada una de las SubCA. Dicho modulo criptográfico o HSM marca Gemalto y modelo Luna K6 Base, posee certificación FIPS 140-2 de hasta nivel 3. Estos dispositivos se encuentran dentro de la categoría de hardware de alta seguridad, los cuales son utilizados por entidades bancarias y de seguridad de estado en todo el mundo, gozando de experiencia y seguridad comprobada.

6.3. Otros aspectos de la gestión de pares de claves.

6.3.1. Archivo de clave pública.

Las claves públicas de las SubCA de Proveedor de Certificados PROCERT, C. A., se archivan en formato PKCS#7, por un periodo de 10 años. El archivo de las claves públicas se ejecuta conforme a lo indicado en el punto 5.5. de esta CPS.

6.3.2. Períodos de funcionamiento del certificado y períodos de uso del par de claves.

Los certificados de las SubCa de Proveedor de Certificados PROCERT, C. A., tendrán una validez de 10 años. Las firmas y los certificados electrónicos generados por cada una de las SubCA de Proveedor de Certificados PROCERT, C. A., tienen un ciclo de un (1) año contado a partir de la fecha de activación del certificado electrónico por parte de la CA de Proveedor de Certificados PROCERT, C. A. El par de claves asociado a cada certificado electrónico tiene igualmente el mismo lapso de vigencia que el certificado del que se trate.

6.4. Datos de activación.

6.4.1. Generación e instalación de datos de activación.

La generación del par de claves (pública y privada) que utilizan las SubCA y sirva a la RPKI de Proveedor de Certificados PROCERT, C. A. es un proceso sencillo, pero que requiere de precauciones especiales. A continuación, se describen los pasos a seguir para la generación del par de

claves y cuáles son las precauciones que deben tomarse a fin de garantizar la protección de la clave privada:

La validación de la identidad del individuo se ejecuta por parte de la RA la cual, una vez creado, registrado y validado el Signatario dentro del Sistema AR, le envía a la CA la información necesaria para que la creación del par de claves del Signatario y de esta forma garantizar la vinculación de identidad de la persona con su par de claves. El Signatario debe ingresar a la página web de PROCERT (http://www.procert.net.ve), dentro del Sistema AR (procert.net.ve/sistemaAR/login.aspx) y presionar click sobre el enlace generación de petición. El sistema indicará que generó su petición de forma correcta. El mismo Sistema AR informa al operador de la AR y CA acerca de la existencia de la petición, la cual una vez validada es aprobada por un encargado de la CA. La aprobación se informa vía correo al Signatario, quien deberá ingresar al Sistema AR a los fines descargar su certificado electrónico.

El signatario al presionar el botón Generar, crea una petición contra la CA y genera su par de claves (pública y privada), esa petición es enviada automáticamente a la RA registro para que sea validada la identidad del Signatario que está realizado la petición de certificado.

El procedimiento de generación de par de claves mencionada garantiza la privacidad de la clave privada del usuario, ya que el usuario es quien la genera, Proveedor de Certificados PROCERT, C. A. solo garantiza la vinculación del individuo con la clave pública, dicha clave pública está asociada a su vez a la clave privada.

Una vez validada la identidad por la AR y generado el certificado por la CA, el Signatario procede a descargar su certificado electrónico en el repositorio de su computadora, aceptando la fuente de emisión del certificado y asignando una clave de uso como requisito dentro de los términos y condiciones de uso.

6.4.2. Protección de datos de activación.
La activación de los certificados emitidos por las SubCA de Proveedor de Certificados PROCERT, C. A. se ejecuta utilizando la RPKI y limitándose en el equipo o dispositivo donde se hayan generado la petición del certificado electrónico por parte del Signatario.

6.4.3. Otros aspectos de los datos de activación.
Ninguno.

6.5. Controles de seguridad informática.
Proveedor de Certificados PROCERT, C. A. posee una política de Seguridad de la Información y un Manual y Modelo de operación de la CA y AR, que establecen y contemplan la ejecución de una serie de procesos orientados al establecimiento de un esquema de prevención, protección y resguardo de la información y los activos informáticos de la RPKI que incluye la CA y la AR. Dentro de las actividades incluidas en la Política de Seguridad de la Información se encuentran las descritas a continuación:

- Creación de un Comité de seguridad y riesgos que establece la gestión de la seguridad de la información como parte fundamental de los objetivos y actividades de Proveedor de Certificados PROCERT, C. A.
- Delimita y establece como debe ser la Conformación del Comité de Seguridad y Riesgo, a los fines de cumplir su objetivo y la debida segregación de roles y funciones.
- Establece cuales son los parámetros y principios que contemplan la contratación de recursos externos que ofrezcan asesoría especializada.
- Clasifica y asigna el control en el manejo de los activos físicos e intangibles.
- Establece los principios aplicables al manejo y seguridad en la gestión del recurso humano.
- Establece los principios aplicables a la seguridad física y ambiental.
- Fija los criterios de control de accesos.
- Fija los criterios aplicables para el establecimiento de contraseñas.
- Protección contra el software malicioso y uso de redes de Proveedor de Certificados PROCERT, C. A.
- Uso compartido de archivos y manejo de información de Proveedor de Certificados PROCERT, C. A.
- Uso establecido pata el correo electrónico interno y externo de Proveedor de Certificados PROCERT, C. A.
- Reglas y protocolos para conexión a Internet.
- Reglas y protocolos para mantenimiento y actualización de software.
- Establecimiento de reglas aplicables a la seguridad perimetral.
- Establecimiento de directrices de acceso a los sistemas y manejo de la CA y RA.
- Regulación del uso de computación móvil y trabajo remoto.
- Reglas para uso aceptable y de asignación de equipos.
- Reglas y procedimientos para el control de cambio en la RPKI incluyendo la CA y la RA.
- Reglas y procedimientos para el mantenimiento t actualización del software de la RPKI y que está diferenciado y separado en CA y RA.
- Reglas y protocolos para el registro, manejo y resguardo de los Logs de evento.
- Reglas, procedimientos y responsabilidades en el manejo y gestión de incidentes.
- Fijación de la debida sincronización de roles.
- Establecimiento de las reglas y procesos que se deben cumplir para la Tercerización y su contratación.
- Establecimiento de los mecanismos de control preventivo para el debido mantenimiento de hardware y software.
- Establecimiento de los principios y reglas para la adquisición, desarrollo y/o mantenimiento de sistemas de información y hardware.
- Reglas, protocolos funciones y roles en la gestión de los riesgos.
- Reglas, protocolos funciones y roles en la gestión de la continuidad del negocio.
- Reglas y funciones para la prevención de código malicioso, spyware y programa maligno.

6.6. Controles técnicos del ciclo de vida.

6.6.1. Controles de desarrollo del sistema.

Proveedor de Certificados PROCERT, C. A. posee una política de Desarrollo de Software, que establecen y contemplan los procesos que deben ser cumplidos para el desarrollo, mantenimiento y pruebas del software de la CA y RA que sea creado dentro de Proveedor de Certificados PROCERT, C. A. En el proceso de generación de software propio Proveedor de Certificados PROCERT, C. A. maneja el establecimiento de distintos ambientes de manejo y prueba de software (desarrollo, calidad y producción) para garantizar el debido funcionamiento y cumplimiento del software de los estándares internacionales establecidos por el CA Browser Fórum y la SUSCERTE para el manejo de una RPKI incluyendo la CA y la RA de Proveedor de Certificados PROCERT, C. A., y en los procesos de puesta en operación de software y sus actualizaciones contemplando los siguientes aspecto:

- Establecimiento del modelo de desarrollo.
- Caracterización del modelo de desarrollo y reglas aplicables al mismos.
- Requisitos para el desarrollador interno o consultor contratado.
- Establecimiento de las actividades que deben ser ejecutadas por el desarrollador.
- Condiciones del entorno de desarrollo.
- Establecimiento de las condiciones y requisitos para aprobación de versiones y certificaciones del software.

6.6.2. Controles de gestión de la seguridad.

Proveedor de Certificados PROCERT, C. A. posee un Manual y Modelo de operación de la CA y un Manuel y Modelo de operación de la RA, los cuales establecen los procesos de seguridad aplicables al manejo y actualización del software que es utilizado para el manejo de la CA y RA. Los manuales antes referidos se orientan a garantizar que los sistemas operativos y el software que sirva a la CA y RA permitan garantizar y mantener su uso esperado, integridad y seguridad.

6.6.3. Controles de seguridad del ciclo de vida.

Proveedor de Certificados PROCERT, C. A. posee una política de Seguridad de la Información y un Manual y Modelo de operación de la CA y un Manual y Modelo de operación de la AR, que establecen y contemplan la ejecución de una serie de procesos orientados al manejo ajustado de la RPKI y de la CA y RA los cuales se encuentran ajustados a las mejores prácticas y lineamientos internacionales dentro de los cuales se encuentran los establecidos por el CA Browser Fórum y la SUSCERTE

6.7. Controles de seguridad de la red.

Proveedor de Certificados PROCERT, C. A. en adición de las actividades contemplada en el aparte 6.5, establece dentro de su política de Seguridad de la Información, Manual y Modelo de operación de la CA y el Manual y Modelo de operación de la AR, el desarrollo de las siguientes actividades:

- Manejo de controles de cambio para actualizaciones, modificaciones o remediaciones dentro de los sistemas y software de la SubCA y RA.
- Debida segmentación y configuración de redes de la RPKI.
- Los certificados de la SubCA se mantienen de forma seguro en dispositivos HSM en centros de datos seguros.
- Actualización recurrente de las contraseñas de acceso a la plataforma y establecimiento de acceso a la SubCA para su gestión y modificación mediante tokens, tarjetas inteligentes y segmentación de roles que de forma concurren permiten la ejecución de determinadas operaciones.
- Protección de la conexión segura entre la SubCA y la AR con el software de gestión de certificados.
- Los certificados de la SubCA se mantienen de forma seguro en dispositivos HSM en centros de datos seguros.
- Protección de conexiones a la SubCA y RA mediante firewalls y configuraciones de red.
- Aplicación de la Política de Seguridad de Información respecto al acceso a la CA, RA y redes y sistemas de Proveedor de Certificados PROCERT, C. A. cumpliendo la debida segmentación de roles y funciones del personal y los Signatarios.
- Debida configuración y mantenimiento de los mecanismos de validación d ellos certificados electrónicos y que están constituido por la LCR y el servicio OCSP.
- Revisión periódica de las conexiones y acceso a puertos de la plataforma que constituyen la RPKI.
- Revisión de la página web de Proveedor de Certificados PROCERT, C. A. a los fines de prevenir y solventar vulnerabilidades.
- Respaldo debido de los registros y procesos de la SubCA y la AR de Proveedor de Certificados PROCERT, C. A.
- Cifrado de información sensible y conexión TLS/SSL entre los distintos servicios de la RPKI.

6.8. Sellado de tiempo.
Proveedor de Certificados PROCERT, C. A., posee una SubCA que emite el certificado para el servicio de estampado de tiempo. Dicha SubCA se encuentra en proceso de certificación y para el momento de emisión de la presente CPS no está activa al público. Una vez la mencionada SubCA cuente con la debida acreditación nacional e internacional se procederá a incluirla como servicio activo en una próxima edición de esta CPS.

7. Perfiles de certificados y CRL.
Proveedor de Certificados PROCERT, C. A., utiliza el estándar ITU X.509, versión 3 para construir certificados digitales para su uso dentro de su RPKI. Proveedor de Certificados PROCERT, C. A., agrega ciertas extensiones de certificado a la estructura básica de certificados para los fines previstos por X.509v3 según la Enmienda 1 de ISO/IEC 9594-8, 1995. Proveedor de Certificados PROCERT, C. A., utiliza una serie de extensiones de certificado para los fines previstos por X.509v3, según la Enmienda 1 de ISO/IEC 9594-8, 1995. X.509v3 es un estándar de la Unión Internacional de Telecomunicaciones para certificados digitales.

7.1. Perfil del certificado.
Los certificados de Proveedor de Certificados PROCERT, C. A., son emitidos conforme a las siguientes normas:

- RFC 6818: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, January 2013
- ITU-T Recommendation X.509 (2016): Information Technology – Open System Interconnection - The Directory: Authentication Framework
- ETSI TS 101 862 V1.3.3 (2006-01): Qualified Certificate Profile, 2006
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March2004 (prevaleciendo en caso de conflicto la TS 101 862).

7.2. Extensiones del certificado:
Las extensiones de los certificados de Proveedor de Certificados PROCERT, C. A., permiten codificar información adicional en los certificados. Las extensiones estándar X.509 definen los siguientes campos: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; y viii) AuthorityInformationAccess.

7.3. Identificación de objeto (OID) de los algoritmos.
El OID del algoritmo criptográfico utilizado por Proveedor de Certificados PROCERT, C. A., es: For P-384 keys, the namedCurve SHALL be secp384r1 (OID: 1.3.132.0.34).

7.4. Formatos de nombres.
Proveedor de Certificados PROCERT, C. A., solo genera y firma certificados de nombres acordes al estándar x 500. Para las SubCA de Proveedor de Certificados PROCERT, C. A.: El nombre distintivo (DN) del está formado por los siguientes atributos:

Subordinada SMIME.
- CN=PROCERT SMIME ECC CA
- O=Proveedor de Certificados PROCERT
- C=VE

El nombre alternativo (AN) de Proveedor de Certificados PROCERT, C. A., está formado por los siguientes atributos.

- DNSName: procert.net.ve.
- otherName:
- OID 2.16.862.2.1. (Código de identificación del PSC PROCERT acreditado)
- OID 2.16.862.2.2.: RIF J- 31635373-7

Para los Subscriptores: El nombre distintivo (DN) del signatario está formado por los siguientes atributos dependiendo de la categoría:

Subscriptor SMIME
Mailbox-validated.
- CN= infoprocert

- E= info@procert.net.ve

Organization-validated.
- CN= Matheu Dilon
- O= Proveedor de Certificados PROCERT, C.A.
- OU= Operaciones
- OI= J316353737 o G200040360
- SERIALNUMBER= V22222222 o P1994455
- E= matheu.dilon@procert.net.net.ve
- ST= Av. Libertador, Multicentro Empresarial del Este
- L= Chacao
- S= Miranda
- POSTALCODE= 1060
- C= VE

Sponsor-validated.
- CN= Matheu Dilon
- O= Proveedor de Certificados PROCERT, C.A.
- OU= Operaciones
- OI= J316353737 o G200040360
- G= Matheu
- SN= Dilon
- SERIALNUMBER= V22222222 o P1994455
- E= matheu.dilon@procert.net.net.ve
- T= Ingeniero en Informatica
- ST= Av. Libertador, Multicentro Empresarial del Este
- L= Chacao
- S= Miranda
- POSTALCODE= 1060
- C= VE

Individual-validated.
- CN= Matheu Dilon
- G= Matheu
- SN= Dilon
- SERIALNUMBER= V22222222 o P1994455
- E= matheudilon@gmail.com
- T= Ingeniero en Informatica
- ST= Calle Bolivar, Chacao, Caracas
- L= Caracas
- S= Miranda
- POSTALCODE= 1060
- C= VE

El nombre alternativo (AN) del signatario está formado por los siguientes atributos:

- otherName: OID 2.16.862.2.2.: (Numero de Cedula de Identidad o Pasaporte)

7.4.1. Necesidad de nombres significativos.

Proveedor de Certificados PROCERT, C. A., requerirá de los clientes contratantes de firmas o certificados electrónicos sus nombres y apellidos completos y conformen figuran representados en la cédula de identidad laminada que posea el solicitante de la firma o certificado electrónico. No serán admitidos o procesados por la RA los datos correspondientes a diminutivos de nombres, alias o seudónimos con los cuales se pretenda identificar el cliente.

En el caso de las poblaciones indígenas serán considerados los nombres que figuran en su cédula de identidad o pasaporte. En todo caso Proveedor de Certificados PROCERT, C. A., garantiza que los DN contenidos en los campos de los certificados son lo suficientemente distintivos y significativos para poder vincular la identidad de un cliente a su firma o certificado electrónico.

7.4.2. Interpretación de formatos de nombre.

Las reglas utilizadas para la interpretación de los nombres distinguidos en los certificados emitidos están descritas en la ISO/IEC 9595 (X.500) DintinguishName (DN). Adicionalmente todos los certificados emitidos por Proveedor de Certificados PROCERT, C. A., utilizan codificación UTF8 para todos los atributos, según la RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, January 2013.

7.4.3. Unicidad de los nombres.

La Autoridad de Certificación de la SUSCERTE define como campo DN del certificado de autoridad como único y sin ambigüedad. Para ello se incluirá como parte del DN, específicamente en el campo OU, el nombre o razón social de Proveedor de Certificados PROCERT, C. A., la unicidad se garantiza mediante la confianza sobre la unicidad de los nombres mercantiles en el registro nacional.

Adicionalmente y respecto a los clientes; si existe un cliente que mantenga contrato y haya adquirido más de un tipo de firma o certificado electrónico, la base de datos de Proveedor de Certificados PROCERT, C. A., mantendrá un esquema uniforme e igualitario de datos del cliente contratante y no será permitido o procesado por la RA, datos personales disimiles y que correspondan a un mismo cliente.

7.4.4. Resolución de conflictos relativos a nombres.

En el caso de una ocurrencia de conflicto de nombre entre clientes y que corresponda a nombre y apellidos iguales, la RA procederá a realizar la distinción de identidad y autenticación de esta a través del uso del número de cédula de identidad y RIF personal de cada cliente de Proveedor de Certificados PROCERT, C. A., con las cuales se haya generado el conflicto de nombre.

Proveedor de Certificados PROCERT, C. A., utilizará la definición de política de asignación de OID’s según el árbol privado de numeración

asignado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

7.5. Perfil de LCR / OCSP:

La lista de certificados revocados (LCR) es una lista de firmas y certificados electrónicos, en la cual concretamente, se muestran los números de serie de las firmas o certificados electrónicos revocados por una CA, los números de serie que han sido revocados ya no son válidos, y por ende el usuario no debe confiar en ningún certificado incluido en la LCR del sistema. Una LCR es un archivo que contiene:

- Nombre del emisor de la LCR;
- Números de serie de la firma o certificado;
- Fecha de revocación de las firmas o certificados,
- La fecha efectiva y la fecha de la próxima actualización y
- La razón de la revocación. Dicha lista está firmada electrónicamente por la propia CA que la emitió.

Cuando un usuario desea comprobar la validez de un certificado debe descargar e instalar la LCR actualizada desde los servidores de la misma CA que emitió el certificado electrónico, al realizar esto, las firmas o certificados que se encuentren instalados en el computador en donde se halla instalado la LCR, automáticamente se validan, si los mismos se encuentran revocados, se invalidan; también se puede comprobar a través del número de serie ubicado en la LCR el status de algún otro certificado.

Se comprueba la autenticidad de la lista gracias a la firma electrónica de la autoridad de certificación.

La estructura de la LCR de Proveedor de Certificados PROCERT, C. A., posee la siguiente estructura, dependiendo la categoría:

General

CAMPO	VALOR
Version	V2
Emisor *Issuer*	CN= [CA Certificate Common Name] O= [CA Certificate Organization] C= [CA Certificate Country Name]
Válido desde	Fecha (UTC)
Válido hasta	Fecha (UTC)
Algoritmo de Firma *signature*	Sha384ECDSA
Algoritmo hash de firma	sha384
EXTENSIONES	
Identificador de clave de entidad emisora *authorityKeyIdentifier* (requerido)	Id. de clave= 4882344ee6311103e6532c8123d14746b5ea946e
Numero de LCR C*RLNumber*	Valor numérico entero

Lista de revocación.

- serialNumber
- revocationDate

Si existe una extensión de entrada de CRL reasonCode, el CRLReason debe indicar el motivo más adecuado para la revocación del certificado, a menos que no se especifique el motivo. El CA Browser Forum TLS especifica los siguientes códigos de motivo de RFC 5280, tabla 83, sección 7.2.2., según corresponda para la mayoría de los casos cuando se utilizan de acuerdo con las prácticas de esta sección y este CPS:

- Unspecified (0)
- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- certificateHold (6)
- privilegeWithdrawn (9)

Proveedor de Certificados PROCERT, C. A., establece que el CRLReason indicado NO DEBE estar sin especificar (0). Si hay una extensión de entrada CRL reasonCode, CRLReason DEBE indicar el motivo más apropiado para la revocación del certificado, las razones de certificación de certificados son las siguientes:

Para Certificados S/MIME.

- keyCompromise: este motivo se utiliza cuando Proveedor de Certificados PROCERT, C. A., ha recibido pruebas o sospechas razonables de compromiso de clave para certificados revocados.
- Compromise: este motivo se utiliza cuando Proveedor de Certificados PROCERT, C. A., ha recibido pruebas o sospechas razonables de compromiso de clave por parte del Signatario.
- AffiliationChanged: esta razón se utiliza cuando el nombre del sujeto u otra información de identidad del sujeto en el certificado ha cambiado
- superseded: esta razón se utiliza cuando el suscriptor ha solicitado un reemplazo o Proveedor de Certificados PROCERT, C. A., ha obtenido información de que la información validada no es confiable y no cumple luego de emitido el certificado electrónico al Signatario.

7.5.1. Número(s) de versión.

El respondedor OCSP de Proveedor de Certificados PROCERT, C. A., cumple con RFC 6960 y 5019.

7.5.2. Extensiones OCSP.

Las extensiones únicas de una respuesta OCSP NO DEBEN contener la extensión de entrada de CRL reasonCode (OID 2.5.29.21). Las extensiones de los certificados del PSC PROCERT permiten codificar información adicional en los certificados.

Las extensiones estándar X.509 definen los siguientes campos: i) SubjectKeyIdentifier; ii) AuthorityKeyIdentifier; iii) BasicConstraints; iv) Certificate Policies; v) KeyUsage; vi) LCRDistribucionPoint; vii) SubjectAlternativeName; y viii) AuthorityInformationAccess.

SMIME.
Las singleExtensions de una respuesta OCSP NO DEBEN contener el reasonCode (OID 2.5.29.21)

8. Auditoría de cumplimiento y otras evaluaciones.
Proveedor de Certificados PROCERT, C. A. en cumplimiento de los estándares internacionales de seguridad de la información, de las previsiones del CA Browser Fórum y de las normas de la SUSCERTE ha establecido un esquema de auditorías anuales y periódicas orientadas y diseñadas a dar cumplimiento a los estándares de industria antes indicado y satisfacer los requerimientos del Programa de WebTrust para una CA abierta.

8.1. Tipos de Auditoría y evaluaciones.
Proveedor de Certificados PROCERT, C. A. dentro de su esquema de auditorías de sistemas y proceso, mantiene una programación anual que contempla la ejecución de auditorías nacionales e internacionales con un régimen anual y trimestral; al igual que otros tipos de evaluaciones orientados a verificar y dar certeza del cumplimiento de estándares de industria. Dichas auditorias y su esquema de aplicación de indican a continuación:

Tipo de Actividad	Cobertura	Frecuencia
Webtrust	Verificación del cumplimiento de los estándares de industria aplicables a CA abiertas que prestan servicios al público en general.	Anual
Auditoria de acreditación ante SUSCERTE	Verificación del cumplimiento de los requisitos establecidos por la SUSCERTE para la operación de un Proveedor de Servicios de Certificación dentro de la República Bolivariana de Venezuela.	Anual
Auditoría de control y seguimiento en seguridad de la información y procesos de la CA.	Auditoría orientada a la verificación del cumplimiento de los mecanismos de control y aseguramiento de operación de una CA, en cumplimiento de los estándares de industria aplicables a CA abiertas que prestan servicios al público en general y que se encentran documentados en la CPS y las políticas de Proveedor de Certificados PROCERT, C. A.	Trimestral
Auditoría de control y seguimiento en procesos administrativos y procesos de la RA.	Auditoría orientada a la verificación del cumplimiento de los mecanismos de control y aseguramiento de operación de una RA, en cumplimiento de los estándares de industria y que se encentran documentados en la CPS y las políticas de Proveedor de Certificados PROCERT, C. A.	Trimestral

Test de penetración	Ejecutado sobre la plataforma y página web de Proveedor de Certificados PROCERT, C. A. y orientado a la detección y determinación de la existencia de vulnerabilidades y aplicación de remediaciones.	Anual

Las auditorias contratadas por Proveedor de Certificados PROCERT, C. A. son ejecutadas por auditores independientes calificados y con obligación de confidencialidad de la información. Igualmente, los mecanismos de evaluaciones se contratan con técnicos debidamente acreditados y calificados a los fines de verificar el cumplimiento de las previsiones de esta CPS y garantizando la seguridad de la información.

8.2. Auditoría y expertos.

Proveedor de Certificados PROCERT, C. A. dentro de su esquema de operación mantiene una política de contratación de servicios que establece la evaluación de la calificación y suficiencia del personal que ejecutará las auditorías y le evaluaciones de los procesos y sistemas de Proveedor de Certificados PROCERT, C. A. En todo caso y para los fines de las auditorías internacionales los auditores deben cumplir con los requisitos de la sección 8.2 de los Requisitos de referencia del foro CAB y la sección 3.1 de la política de Mozilla Root Store cuando corresponda. Para la auditoría ante la SUSCERTE los auditores deben contar con su número de identificación de auditor acreditado ante la SUSCERTE. Palas demás evaluaciones se procederá con un proceso de selección basado en las calificaciones y recomendaciones de industria para la ejecución de auditorías de tercera parte independientes. Los auditores deben suscribir un contrato de confidencialidad y uno de servicio y se verificará bajo juramento que no guardan un interés directo financiero o comercial en las resultas de la auditoría o poseen relación familiar con personal o directivos de Proveedor de Certificados PROCERT, C. A. en segundo grado de consanguinidad y cuarto grado de afinidad.

8.3. Alcance de las auditorías y evaluaciones.

El alcance de las auditorias y las evaluaciones se orientan al cumplimiento por parte de Proveedor de Certificados PROCERT, C. A. de las previsiones y obligaciones que bajo estándar debe tener una CA comercial bajo los principios de esta CPS y del CA Browser Fórum, el Webtrust, el estándar ETSI y las normas de seguridad de información que orienta al funcionamiento esperado de la RPKI y del cumplimiento por parte de Proveedor de Certificados PROCERT, C. A. de sus obligaciones comerciales y legales.

8.4. Informes de auditoría y cumplimiento.

Proveedor de Certificados PROCERT, C. A. gestionará los informes de auditoría o evaluaciones conforme al plan de auditoría o trabajo establecido antes de cada uno de los procesos indicados en el punto 8.1. El plan de remediación será elaborado con acuerdo entre el auditor y el personal de Proveedor de Certificados PROCERT, C. A. y debe fijar los puntos de revisión y mejora, los cuales quedarán documentados y presentados a los fines de su subsanación antes de la finalización de la auditoría o dentro del plazo establecido por el auditor a tal fin. El caso del Webtrust los informes de auditoría estará a disposición de los terceros interesados a través del enlace

https://www.procert.net.ve/Internas/AC.aspx En el caso de la auditoría de SUSCERTE el informe de acreditación se encuentra en los repositorios de seguridad de Proveedor de Certificados PROCERT, C. A. En el caso de las evaluaciones de seguridad, las mismas serán tratadas de conformidad con lo establecido en la Política de Seguridad de la Información de Proveedor de Certificados PROCERT, C. A.

9. Otros asuntos comerciales y legales.
Esta sección se orienta al establecimiento de los aspectos comerciales y legales de la operación de Proveedor de Certificados PROCERT, C. A. con sus Signatarios y entidades finales usuarias de certificados electrónicos emitidos por la SubCA de Proveedor de Certificados PROCERT, C. A.

9.1. Tarifas.
Las tarifas y cargos asociados a la prestación de los servicios y emisión d ellos certificados de Proveedor de Certificados PROCERT, C. A. contemplan el total de inversión que requiere un Signatario o entidad final usuaria de certificados electrónicos, para la adquisición de un certificado electrónico o servicio de TSA y su uso conforme estándar por un período de un (1) año. Las tarifas de los certificados y servicios de Proveedor de Certificados PROCERT, C. A. pueden ser consultados a través del siguiente enlace: https://www.procert.net.ve/

Proveedor de Certificados PROCERT, C. A. efectúa una revisión periódica del costo de sus certificados electrónicos y servicios, a los fines de mejorarlos en caso de ser posible y hacer más asequible sus servicios y sus certificados para sus Signatarios y entidades finales usuarias de certificados electrónicos.

Dentro de su esquema tarifario Proveedor de Certificados PROCERT, C. A. contempla acciones de re4sponsabilidad social de empresa, orientados a grupos o entidades que requieren acción social y compromiso de empresa con el entorno.

9.1.1. Tasas de emisión o renovación de certificados.
Proveedor de Certificados PROCERT, C. A. contempla en su estructura tarifaria un pago único por Signatario por suscripción no transferible, la cual puede ser dividida en pagos mensuales domiciliados. Las tarifas de los certificados y servicios de Proveedor de Certificados PROCERT, C. A. pueden ser consultados a través del siguiente enlace: https://www.procert.net.ve/

9.1.2. Tarifas de acceso a certificados.
Proveedor de Certificados PROCERT, C. A. cobra una tarifa accesible y razonable por el acceso a la base de datos de sus certificados, uso de sus certificados electrónicos, servicio de TSA y servicios profesionales.

9.1.3. Revocación o Tarifas de Acceso a la Información de Estado [OMITIDO]
Proveedor de Certificados PROCERT, C. A. no contempla el cargo conceptos o establecimiento de tarifas por el uso de sus servicios de comprobación del ciclo de vida de los certificados como la LCR y el OCSP. Tampoco se establecen cargos o costos por la revocación de los certificados

o la comprobación de Signatarios a través del enlace https://www.procert.net.ve/ConsultaPublica/index.aspx

9.1.4. Tarifas por otros servicios.

Proveedor de Certificados PROCERT, C. A. no contempla cargos o costos adicionales por el acceso a los validadores del ciclo de vida de los certificados o por la documentación de CPS o CP de la RPKI. Servicios profesionales de implantación y configuración en sistemas de certificados electrónicos no están incluido dentro de la tarifa del certificado y deben ser solicitados por separado.

9.1.5. Política de reembolso.

Los Signatarios de Proveedor de Certificados PROCERT, C. A. solo pueden solicitar el reembolso de la tarifa pagada por su certificado antes de la gestión del certificado y aprobación de su certificado por la AR a través de la conformación del expediente electrónico del Signatario en el Sistema AR de Proveedor de Certificados PROCERT, C. A. La solicitud de reembolso debe ser efectuada a través del correo soporte@procert.net.ve

9.2. Responsabilidad financiera.

9.2.1. Cobertura del seguro.

Los límites de la responsabilidad de Proveedor de Certificados PROCERT, C. A. hacia sus Signatarios está regulada mediante acuerdos contractuales con dichas clientes. La responsabilidad de Proveedor de Certificados PROCERT, C. A. para con los Signatarios y cualquier otra entidad final usuaria de certificados electrónicos generados por Proveedor de Certificados PROCERT, C. A., está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas con dicho certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa. Todos y cada uno de los reclamos que surjan de la RPKI de Proveedor de Certificados PROCERT, C. A. con relación a un certificado (sin reparar en la entidad causante de los daños), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con esta CPS y la CP.

9.2.2. Otros activos.

Sin estipulaciones.

9.2.3. Cobertura de seguro o garantía para entidades finales.

Sujeto a las limitaciones indicadas en 9.2.1., el límite de responsabilidad agregada de la CA de Proveedor de Certificados PROCERT, C. A. hacia todos los Signatarios, ni por todo el período de validez de un certificado emitido por Proveedor de Certificados PROCERT, C. A. hacia todas las personas con relación a dicho certificado es de quince mil unidades tributarias (15.000 U.T.) de la República Bolivariana de Venezuela. En ningún caso la responsabilidad de la CA excederá el límite antes mencionado.

9.3. Confidencialidad de la información comercial.

9.3.1. Alcance de la información confidencial.

Proveedor de Certificados PROCERT, C. A. mantiene previsiones de confidencialidad de la información y acceso a la información en los contratos con los Signatarios, mantiene una política de confidencialidad y un plan de confidencialidad de la información a los fines de asegurar información sensible de personas no autorizadas identificando cierta información como confidencial y por ende no accesible a personal que no sea de confianza. La información que se cataloga como confidencial es la siguiente:

1. Acceso a claves privadas;
2. Datos de activación utilizados para acceder a las claves privadas o para obtener acceso al sistema AR;
3. Planes de continuidad del negocio, respuesta a incidentes, contingencia y recuperación ante desastres;
4. Esquemas y procedimientos de seguridad utilizados para proteger los datos, la confidencialidad, integridad y disponibilidad de la información;
5. Registros de auditoría interna.
6. Registro de logS de los sistemas que conforma la RPKI incluyéndola CA y la AR.
7. Registros financieros y de auditorías financieras.
8. Registros de archivo de información clasificada como confidencial.
9. Información de los Signatarios.
10. Procedimientos y planes de recuperación ante desastres.
11. Procedimientos internos sobre manejo y configuración de la RPKI que incluye la CA y la RA.
12. Manejo de claves y controles de acceso.
13. Toda aquella información que posea una reserva legal de confidencialidad.

9.3.2. Información que no entra en el ámbito de la información confidencial.

Proveedor de Certificados PROCERT, C. A. informa que no considerará como confidencial la siguiente información:

1. La CPS y la CP.
2. Todos los certificados emitidos por la RPKI, para uso público pueden ser divulgados públicamente.
3. Todos los certificados revocados.
4. Toda información que no posea la denominación de privada y confidencial.

9.3.3. Responsabilidad de proteger la información confidencial.

Proveedor de Certificados PROCERT, C. A. mantiene previsiones de confidencialidad de la información y acceso a la información en los contratos con los Signatarios, mantiene una política de confidencialidad y un plan de confidencialidad de la información los cuales establecen responsabilidad de los representantes y empleados de Proveedor de Certificados PROCERT, C. A. con relación al manejo, protección, uso y resguardo de la información confidencial de los Signatarios y de la operación completa de la RPKI; siendo instruidos al respecto y acerca de sus responsabilidades legales por manejo y uso no autorizado de la información confidencial.

9.4. Privacidad de la información personal.

9.4.1. Plan de privacidad.

Proveedor de Certificados PROCERT, C. A. mantiene una política de confidencialidad y un plan de confidencialidad de la información los y en los contratos de trabajo y de servicio con sus empleados y proveedores establecen mecanismos de protección y resguardo de la información. Proveedor de Certificados PROCERT, C. A. mantiene en su página web una política de privacidad a la cual se accede a través https://www.procert.net.ve/Docs/Pol%C3%ADtica%20Privacidad.pdf. La información de los Signatarios solo podrá ser divulgada mediante orden judicial debidamente librada por una autoridad judicial y en cumplimento de los extremos legales pertinentes.

9.4.2. Información tratada como privada.

Proveedor de Certificados PROCERT, C. A. establece en sus políticas internas y el contrato con sus Signatarios que toda la información recibida en el proceso de contratación de un certificado electrónico será tratada como información privada de los Signatarios y en consecuencia tendrá una protección en cuanto a su uso. acceso no autorizado, publicación.

9.4.3. Información no considerada privada.

Los datos y registros de publicación de certificados y sus validadores del ciclo de vida de los certificados, como lo son la LCR y el OCSP, no son datos privados.

9.4.4. Responsabilidad de proteger la información privada.

Proveedor de Certificados PROCERT, C. A. establece que es responsabilidad de sus empleados y proveedores el manejar de forma adecuada la información privada y cumplirá tales efectos las previsiones contenidas en sus contratos de trabajo y servicio, garantizando en todo momento la privacidad del dato de los Signatarios y de Proveedor de Certificados PROCERT, C. A. Toda la información considerada como privada es resguardada siguiendo las directrices de la política de seguridad de la información de Proveedor de Certificados PROCERT, C. A. Proveedor de Certificados PROCERT, C. A. , sus empleados y proveedores están obligados igualmente a cumplir la legislación nacional e internacional en materia de manejo de datos privados de los Signatarios.

9.4.5. Aviso y consentimiento para el uso de información privada.

Proveedor de Certificados PROCERT, C. A., mantiene una política de resguardo y protección de la información Privada de los Signatarios, la cual solo será posible revelar con motivo de una orden judicial firme emanada por una autoridad competente y previamente informada al Signatario. Proveedor de Certificados PROCERT, C. A., puede determinar sin consentimiento de los Signatarios si un certificado se encuentra activo o revocado.

9.4.6. Divulgación de conformidad con un proceso judicial o administrativo.

Con base a lo establecido en el contrato de suscripción con los Signatarios y los contratos con contratistas, Proveedor de Certificados PROCERT, C. A., establece la potestad de compartir los datos privados de los

Signatarios o información de contrato con proveedores, siempre que medie una orden judicial efectiva y firme y limitada a los datos requeridos para la creación de un certificado electrónico.

9.4.7. Otras circunstancias de divulgación de información.
No hay otras estipulaciones.

9.5. Derechos de propiedad intelectual (si corresponde).
Proveedor de Certificados PROCERT, C.A. Todos los derechos reservados; el logo de Proveedor de Certificados PROCERT, C.A. y los nombres de los productos son marcas comerciales de Proveedor de Certificados PROCERT, C.A., sus desarrollo, aplicaciones y software especializado. Excepto por los componentes que pueden ser propiedad intelectual de Terceros, todos los derechos de propiedad intelectual, incluyendo los derechos de autor en todos los directorios de certificados, listas de LCR y certificados; a menos que explícitamente se indique lo contrario, todas las prácticas, política, los documentos operacionales y de seguridad referentes a la RPKI (electrónicos o no) así como los contratos, le pertenecen y seguirán siendo propiedad de Proveedor de Certificados PROCERT, C.A. Mediante los contratos correspondientes para la prestación de servicios de certificación, Proveedor de Certificados PROCERT, C.A. podrá otorgar una licencia a terceros para el uso de certificados, LCR y otras prácticas autorizadas y documentos de política en la medida que lo requieran para la prestación de servicios de certificación de acuerdo con el presente documento de la CPS y CP.

9.6. Declaraciones y garantías.

9.6.1. Declaraciones y garantías de CA.
Proveedor de Certificados PROCERT, C.A. declara que no hace declaraciones respecto a los certificados electrónicos que genera y los servicios que prestan en general salvo las relacionadas con el funcionamiento y uso de dichos certificados y servicios y que se indican a continuación:

- Proveedor de Certificados PROCERT, C.A. cumple con sus obligaciones de conformidad con los establecido en el CA Browser Fórum y las normas de la SUSCERTE.
- Proveedor de Certificados PROCERT, C.A. Cumple con mantener disponibles y activos los mecanismos de validación de vida de los certificados electrónicos como lo son la LCR y el OCSP.
- Proveedor de Certificados PROCERT, C.A. Cumple con mantener disponibles y en funcionamiento su RPKI.
- Proveedor de Certificados PROCERT, C.A. cumple con las previsiones, procedimientos y declaraciones contenidas en la CPS y la CP.
- Proveedor de Certificados PROCERT, C.A. cumple con las previsiones y obligaciones contemplados en el contrato de servicio suscrito con sus Signatarios.
- Proveedor de Certificados PROCERT, C.A. cumple con el ordenamiento legal que regula el funcionamiento de un Proveedor de Servicios de Certificación dentro de la República Bolivariana de Venezuela.

- Proveedor de Certificados PROCERT, C.A. Cumple con mantener mecanismos de información a los Signatarios en caso de compromiso de clave privada o cese de operación
- Proveedor de Certificados PROCERT, C.A. Cumple con mantener disponibles y activos los mecanismos de generación de certificados electrónicos a través del Sistema AR.
- Proveedor de Certificados PROCERT, C.A. Cumple con mantener las fianzas que exige la SUSCERTE.

9.6.2. Declaraciones y garantías del suscriptor.

Proveedor de Certificados PROCERT, C.A. declara que no hace declaraciones respecto a los certificados electrónicos que genera y los servicios que prestan en general salvo las relacionadas con el funcionamiento de los mecanismos de comprobación de la RA y que se indican a continuación:

- Proveedor de Certificados PROCERT, C.A. cumple a los efectos de la RA con sus obligaciones de conformidad con los establecido en el CA Browser Fórum y las normas de la SUSCERTE.
- Proveedor de Certificados PROCERT, C.A. Cumple con mantener disponibles y activos los mecanismos de validación AR.
- Proveedor de Certificados PROCERT, C.A. cumple con las previsiones, procedimientos y declaraciones de RA contenidas en la CPS y la CP.
- Proveedor de Certificados PROCERT, C.A. cumple con las previsiones y obligaciones contemplados en el contrato de servicio suscrito con sus Signatarios.
- Proveedor de Certificados PROCERT, C.A. cumple con el ordenamiento legal que regula la actividad de la RA dentro de la República Bolivariana de Venezuela.
- Proveedor de Certificados PROCERT, C.A. cumple a los efectos que la RA mantenga los mecanismos de comprobación y validación de la identidad.
- Proveedor de Certificados PROCERT, C.A. cumple a los efectos de que la información procesada por la RA se maneje y se mantenga con un criterio de confidencialidad y privacidad de la información.
- Proveedor de Certificados PROCERT, C.A. ®. cumple a los efectos de garantizar que la RA mantenga expedientes electrónicos de los Signatarios.

9.6.3. Declaraciones y garantías de la parte que confía.

Proveedor de Certificados PROCERT, C.A. declara que no hace declaraciones respecto a los certificados electrónicos que genera y los servicios que prestan en general y que, bajo el contrato suscrito, los Signatarias hacen las declaraciones que se indican a continuación:

- Utilizar el certificado para el fin para el cual fue contratado.
- Cumplir los términos y condiciones de uso del contrato que regula el certificado electrónico contratado.

- Cumplir la legislación vigente dentro de la República Bolivariana de Venezuela.
- Generar su par de claves.
- Asignar una clave de uso para el certificado conforme al manual de uso y descarga del certificado electrónico.

9.7. Renuncias de garantías.
Proveedor de Certificados PROCERT, C.A. declara que existe una CP que establece el uso de cada uno de los certificados electrónicos que genera; dicha CP establece los usos autorizadnos y no autorizados; igualmente describe al certificado su alcance, plataforma que la soporta, fijando de esa manera el uso y funcionamiento esperado de los certificados. De esta forma Proveedor de Certificados PROCERT, C.A. limita su responsabilidad a la establecida en la CPS y CP fijándose tal situación en los términos y condiciones contenidos en el contrato de uso que suscribe y acepta el Signatario.

9.8. Limitaciones de responsabilidad.
Proveedor de Certificados PROCERT, C.A. declara que no asumirá la responsabilidad de datos y procedimientos que no se encentren contemplados y señalados en los términos y condiciones del contrato suscrito por el Signatario

9.8.1. Cumplimiento requisitos legales.
Proveedor de Certificados PROCERT, C.A. declara que no asumirá la responsabilidad de datos y procedimientos que no se encentren contemplados y señalados en la norma legal aplicable decreto ley sobre mensajes de datos y firmas electrónicas (LSMDFE), el reglamento (RLSMDFE) y la normativa de la SUSCERTE, dentro de esos procedimientos, garantías y procesos se enuncian los siguientes:

- La de alcanzar resultados específicos.
- De comerciabilidad o idoneidad para un propósito específico,
- Con relación a la exactitud o confiabilidad de la información contenida en los Certificados que no sean suministrados y/o verificados por la RA.
- Que no están relacionadas con los temas cubiertos por esta CPS y la CP.
- Sobre la responsabilidad o estabilidad comercial o financiera de terceros que suministren los servicios de certificación bajo su propia autoridad o usando o dependiendo de los servicios de certificación, en los casos de doble certificación;
- Sobre la validez jurídica, la capacidad de satisfacer requerimientos formales o el estatus de prueba de las firmas electrónicas, certificados o claves criptográficas y
- Con relación a los asuntos fuera del control razonable de la CA.
- Si la CA es responsable de su incumplimiento con las garantías o por cualquier otra razón, se procederá la indemnización contemplada en la fianza establecida por la SUSCERTE, no obstante se observará en todo momento que el pago de daños excesivos que se pretendan fijar no aplicarán para aquellas actividades que no están directamente relacionadas con las condiciones de los servicios de certificación (de la

misma manera que una autoridad pública no puede ser responsable por lo que una persona haga con una “Firma Electrónica”). La CA por lo tanto requiere que los miembros de la comunidad de la RPKI consientan con el hecho que Proveedor de Certificados PROCERT, C.A. no asume responsabilidad por ningún tipo de daños que surjan de las circunstancias descritas más abajo (incluyendo daños especiales, consecuentes, incidentales, indirectos o punitivos), sin importar que haya sido notificada de ellos (o de su potencialidad) o no, o si éstos son razonablemente previsibles o no.

- Transacciones subyacentes entre los clientes y terceros, incluyendo las partes dependientes;
- Los servicios y/o productos de Terceros (incluyendo el hardware y software) que interactúan o usan los servicios de certificación, certificados, firmas electrónicas, etc.;
- Si existe un retraso, mutilación, o pérdida u otros errores en relación con los datos o documentos mientras son creados, almacenados o comunicados;
- Dependencia inaceptable de un Certificado, una firma electrónica, una clave criptográfica o par clave, o los servicios de certificación a los cuales se refiere esta CPS y la CP;
- Incumplimiento de terceros (incluyendo miembros de la comunidad de RPKI de Proveedor de Certificados PROCERT, C.A.) con protección de datos local o legislación sobre privacidad, legislación sobre protección al consumidor o cualquier otro cumplimiento legislativo o regulatorio requerido por la jurisdicción local; o
- Cualquier daño indirecto o consecuente, perdida de utilidades, pérdida plusvalía, pérdida de ahorros estimados, pérdida de ganancias, pérdida de negocios, interrupción de negocios; o pérdida de información.
- Para mayor protección de los riesgos relacionados con la condición de servicios de certificación y para garantizar la estabilidad a largo plazo de la RPKI, el monto de cualquier daño reconocido también está limitado bajo las condiciones fijadas en la póliza de seguro requerida por la SUSCERTE para la operación de Proveedor de Certificados PROCERT, C.A.

9.8.2. Limitaciones de pérdidas.

Los límites de la responsabilidad de Proveedor de Certificados PROCERT, C.A. hacia los Signatarios, está regulada mediante acuerdos contractual. Como referencia a estos contratos se incorporan esté documento de la CPS y CP y las demás políticas de acreditación elaboradas por el Proveedor de Certificados PROCERT, C.A. y referidas en la Política de Seguridad de la Información de ésta.

A menos que se haya acordado explícitamente o se haya incorporado explícitamente en un certificado, la responsabilidad de Proveedor de Certificados PROCERT, C.A. para con los clientes, proveedores o parte interesada, está limitada contra reclamos de cualquier tipo, incluyendo los contractuales, ilegales, extra contractual y de naturaleza delictiva, en cada certificado en particular sin importar el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas con dicho

certificado o cualquier servicio prestado con respecto a dicho certificado y en forma acumulativa.

Todos y cada uno de los reclamos que surjan de la RPKI con relación a un certificado (sin reparar en la entidad causante de los daños o en la entidad que emitió el certificado o suministró los servicios de certificación), estarán sujetos a los límites de responsabilidad aplicables a éstos de acuerdo con este documento de la CPS y la CP. La responsabilidad máxima por certificado de la RPKI se establecerá en el certificado correspondiente.

Este límite de responsabilidad por certificado aplicará sin reparar en el número de transacciones, firmas electrónicas o causas de acción que surjan o estén relacionadas a dicho certificado o cualquier servicio suministrado con respecto a dicho certificado y sobre una base acumulativa. sujeto a las limitaciones anteriores, el límite de responsabilidad agregada de la CA de Proveedor de Certificados PROCERT, C.A. hacia todos los Signatarios es de quince mil unidades tributarias (15.000 U.T.). En ningún caso la responsabilidad excederá el límite antes mencionado.

9.9. Indemnizaciones.

Toda indemnización será producto de un proceso de investigación y análisis o de resolución de conflictos a través de la vía administrativa o judicial definitivamente firme y donde de forma comprobada de determine la responsabilidad de Proveedor de Certificados PROCERT, C.A. derivada de negligencia o impericia.

9.10. Plazo y rescisión.

9.10.1. Plazo.

Proveedor de Certificados PROCERT, C.A. mantiene una política de gestión documental que establece una revisión de todas las políticas y documentación de empresa cada seis (6) meses o cuando ocurran cambios que lo ameriten: y mediante la cual se actualiza la documentación por revisión de su actualización, modificaciones normativas y legales, actualización de estándares aplicables, entre otros puntos. Se mantiene un registro en la documentación para informar los números de ediciones y versiones de cada documento, dentro de los mismos documentos de Proveedor de Certificados PROCERT, C.A.

9.10.2. Rescisión.

La política de gestión documental de Proveedor de Certificados PROCERT, C.A. establece que la documentación incluyendo la CPS y la CP, estarán vigente hasta tanto requieran modificaciones o actualizaciones derivadas de cambios que lo ameriten y revisiones basadas en su verificación semestral, por cambios normativos y legales, o por orden judicial si es el caso.

9.10.3. Efecto de la rescisión y supervivencia.

Proveedor de Certificados PROCERT, C.A. declara que el cambio de la CPS o la CP y la emisión de una versión o edición posterior a la vigente cuando un Signatario adquirió un certificado, no afectará las condiciones y términos de servicios contratados con PROCERT bajo estándar de la

CA Browser Fórum o de la SUSCERTE y tampoco afectará el lapso de vigencia del certificado. En todo caso se aplicarán las siguientes condiciones:

- Proveedor de Certificados PROCERT, C.A. mantendrá las estipulaciones contenidas en el contrato que mantiene con sus Signatarios.
- Proveedor de Certificados PROCERT, C.A. mantendrá las garantías exigidas por SUSCERTE para la operación como Proveedor de Servicios de Certificación, salvo que, por vía de cambio en CA Browser Fórum, las normas SUSCERTE o medida judicial firma, se establezca una modificación en dichas garantías, siendo necesaria la debida participación e información por parte de Proveedor de Certificados PROCERT, C.A. a sus Signatarios, acerca de los cambios operados.
- Proveedor de Certificados PROCERT, C.A. informará debidamente a sus Signatarios acerca de los cambios en ediciones o versiones de la CPS y la CP.
- Proveedor de Certificados PROCERT, C.A. mantendrá las obligaciones de confidencialidad y manejo de la información privada, salvo que, por vía de cambio en CA Browser Fórum, las normas SUSCERTE o medida judicial firma, se establezca que dicha información ya no reviste carácter confidencial o privado.
- Proveedor de Certificados PROCERT, C.A. informará debidamente a sus Signatarios acerca de cambios en los algoritmos de firma que por cambios y debidos cumplimientos de estándar CA Browser Fórum o las normas SUSCERTE, sea requerido efectuar; en cuyo caso los Signatarios deberán revocar su certificado electrónico, previa emisión por parte de Proveedor de Certificados PROCERT, C.A. de un nuevo certificado electrónico que contemple el plazo restante del periodo contratado por el Signatario del cual se trate.

9.11. Avisos individuales y comunicaciones con los participantes.

Proveedor de Certificados PROCERT, C.A. informa que toda información aviso, solicitud de cambio o revisión de la CPS y la CP podrán ser enviados mediante correo electrónico firmado, el cual debe contar con los datos completos del solicitante incluyendo, nombres y apellidos, número de cédula de identidad o documento de identidad, dirección completa incluyendo código postal, teléfono contacto y dirección electrónica valida. Se emitirá un acuse de recibo generado por el servidor y manejador de correo electrónico de Proveedor de Certificados PROCERT, C.A. Una vez recibida la información Proveedor de Certificados PROCERT, C.A. contará con un lapso de diez (10) días hábiles, dentro de los cuales se dará respuesta a la información o aviso recibido. La respuesta será efectuada mediante correo electrónico firmado y que contendrá acuse de recibo y lectura. Una vez recibida la respuesta de parte de Proveedor de Certificados PROCERT, C.A, el Signatario o remitente del aviso o información deberá dar respuesta respecto a la recepción de la respuesta de Proveedor de Certificados PROCERT, C.A. dentro de los tres (3) días siguientes a su recepción, con lo cual se dará por finalizado el proceso.

9.12. Modificaciones.

9.12.1. Procedimiento de modificación.

Proveedor de Certificados PROCERT, C.A. establece que cualquier cambio de la presente CPS o la CP, es ejecutado conforme a lo establecido en la política de gestión documental de Proveedor de Certificados PROCERT, C.A., la cual establece una revisión de todas las políticas y documentación de empresa cada seis (6) meses o cuando ocurran cambios que lo ameriten como se indicó en el punto 9.10.1. Las actualizaciones deben cumplir el proceso de autorización por parte de las autoridades de Proveedor de Certificados PROCERT, C.A. y serán informadas debidamente a los Signatarios; siendo reemplazadas de forma automática en el repositorio de documentación de Proveedor de Certificados PROCERT, C.A., incluyendo las nuevas versiones de la CPS y la CP. El enlace de consulta de las versiones vigentes y actualizadas de la CPS y la CP se encuentra a disposición de los Signatarios en el enlace https://www.procert.net.ve/Internas/AC.aspx.

9.12.2. Mecanismo y plazo de notificación.

Proveedor de Certificados PROCERT, C.A. establece que cualquier cambio de la presente CPS o la CP, es informado debidamente vía correo electrónico a los Signatarios y publicado en el enlace https://www.procert.net.ve/Internas/AC.aspx. en la página web de Proveedor de Certificados PROCERT, C.A. www.procert.net.ve

9.13. Disposiciones sobre resolución de disputas.

Proveedor de Certificados PROCERT, C.A. contempla en el contrato que mantiene con sus Signatarios una cláusula de resolución de diferencias o disputas, la cual establece que si la controversia no se ha resuelto a través de la negociación entre Proveedor de Certificados PROCERT, C.A. y el Signatario o parte reclamante, dentro de los quince (15) días hábiles después de iniciada la reclamación, entonces a solicitud del Signatario o reclamante se someterá la controversia a la SUSCERTE, ente rector en la materia de certificación electrónica dentro de la República Bolivariana de Venezuela, en virtud de lo establecido en el numeral 13 del artículo 22 el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas. La solución alcanzada con la mediación de SUSCERTE y acepada por Proveedor de Certificados PROCERT, C.A. y el Signatario o parte reclamante, será vinculante y de obligatorio cumplimiento. Proveedor de Certificados PROCERT, C.A. y el Signatario o parte reclamante estarán igualmente en liberad de acudir al organismo encardo de la protección, educación y defensa del usuario contratante conforme a la Ley que regula la materia. En caso de no llegar a ningún acuerdo quedará libre la vía de reclamo por proceso ordinario judicial por ante los Tribunales de la Jurisdicción del área Metropolitana de Caracas con exclusión de cualquier otro.

9.14. Legislación aplicable.

La presente CPS y la CP se regirán e interpretaran de conformidad con lo establecido en la normas del CA Browser Fórum, la normativa de la SUSCERTE para la operación de los Proveedores de Servicios de Certificación y la legislación aplicable al a materia dentro de la República Bolivariana de Venezuela, fijándose como domicilio especial con exclusión de cualquier otro a la ciudad de

Caracas a la jurisdicción de cuyos tribunales los Signatarios acuerdan someterse con exclusión de cualquier otro.

9.15. Cumplimiento de la legislación aplicable.

Proveedor de Certificados PROCERT, C.A. y los Signatarios se obligan a cumplir a los fines de la prestación del servicio los lineamientos y procesos establecidos en la CPS y la CP y en la legislación que regula la materia de certificados electrónicos dentro de la República Bolivariana de Venezuela.

9.16. Disposiciones varias.

9.16.1. Acuerdo completo.

La presente CPS y la CP contienen la totalidad de las condiciones, procesos y acuerdos contractuales sobre los cuales Proveedor de Certificados PROCERT, C.A. contempla la operación de su RPKI dentro de la República Bolivariana de Venezuela; a los fines de la emisión de los certificados electrónicos, la validación de identidad de los Signatarios por parte de la AR, el manejo del ciclo de vida de los certificados, el manejo de la información y los mecanismos de aseguramiento de operación sobre los cuales, los Signatarios aceptan y convienen el uso de certificados electrónicos generados por Proveedor de Certificados PROCERT, C.A. y sobre los cuales está se obliga. Lo no contemplado en la CPS y CP no constituye base del servicio contratado por el Signatario y por ende no será exigible a Proveedor de Certificados PROCERT, C.A.

9.16.2. Cesión.

La presente CPS y las obligaciones que establece hacia los Signatarios podrá ser cedida a otras entidades que asuman por transferencia, venta, fusión o contrato la operación de la RPKI de Proveedor de Certificados PROCERT, C.A. incluyendo las actividades de la CA y AR dentro de la República Bolivariana de Venezuela. Las cesiones de esta CPS en otras entidades no serán efectivas si se constituyen de novaciones de deuda o de fraudes a la Ley.

9.16.3. Divisibilidad.

Proveedor de Certificados PROCERT, C.A. establece que si alguna parte de la CPS se declara invalida, nula o inaplicable por incumplimiento del CA Browser Fórum, las normas de SUSCERTE o por una sentencia firme de un tribunal de la República Bolivariana de Venezuela, se procederá de conformidad con lo establecido en el punto 9.10.1., informando debidamente a los Signatarios y reemplazando las ediciones y versiones sustituidas por la vigente. El enlace de consulta de las versiones vigentes y actualizadas de la CPS y la CP se encuentra a disposición de los Signatarios en el enlace https://www.procert.net.ve/Internas/AC.aspx. No se mantendrán publicaciones de la CPS o CP con parciales nulas o inaplicables y en la eventualidad de no haber sido reemplazadas por las vigentes se indicará con un mansaje dentro de la CPS o CP las partes que no sean aplicables.

9.16.4. Ejecución (honorarios de abogados y renuncia de derechos).

Proveedor de Certificados PROCERT, C.A. que todas y cada una de las partes que integran la presente CPS y la CP se encuentran vigentes y

aplicables, si por alguna razón Proveedor de Certificados PROCERT, C.A. o el Signatario no ejercen su derecho establecido dentro de la CPS o la CP, no se entenderá esto como una renuncia de los derechos que les asisten conforme a la Ley. Ninguna renuncia de derechos será válida sin constar previamente por escrito. Igualmente, Proveedor de Certificados PROCERT, C.A. se reserva el derecho de ejercer acciones y cobros de honorarios en contra de personas que hayan actuado en contra de las previsiones de la CPS o la CP, causando un daño, pérdidas o costos asociados a la atención y remediación de situaciones derivadas de las mencionadas acciones.

9.16.5. Fuerza mayor.

Proveedor de Certificados PROCERT, C.A. quedará relevado de sus responsabilidades por incumplimiento involuntario total o parcial, definitivo o temporal de sus obligaciones bajo la presente CPS y la CP, cuando las mismas se deban a causa que no pueda ser imputada a Proveedor de Certificados PROCERT, C.A., que fuera imprevisible, inevitable y cuyo acaecimiento implique una imposibilidad absoluta para Proveedor de Certificados PROCERT, C.A. de cumplir con las obligaciones asumidas bajo la presente CPS o la CP, bien porque el incumplimiento se deba a:

- Caso fortuito o fuerza mayor, entendiendo como tal aquellos acontecimientos imprevisibles e inevitables que impiden el cumplimiento de la obligación de manera absoluta y que son totalmente independientes de la conducta de Proveedor de Certificados PROCERT, C.A. y que no pueden ser imputados a la misma;
- Al hecho del tercero se entenderán como tales aquellos hechos causados por personas totalmente independientes a Proveedor de Certificados PROCERT, C.A. que impidan a la misma el cumplimiento de sus obligaciones bajo la presente orden de servicio;
- Al hecho del príncipe se debe entender como tal a cualquier disposición legal o sub-legal emanada de órganos competentes del estado y que afecten o regulen la actividad de Proveedor de Certificados PROCERT, C.A. y que de manera absoluta impidan el cumplimiento de las obligaciones contraídas por Proveedor de Certificados PROCERT, C.A. bajo la presente CPS ola CP; y
- La pérdida de la cosa debida cuando la obligación sea la entrega de una cosa cierta y determinada y la pérdida no sea imputable a Proveedor de Certificados PROCERT, C.A., se entenderá como tal, cuando la responsabilidad de Proveedor de Certificados PROCERT, C.A. perezca, desaparezca o se haga insuficiente para los efectos de la presente CPS o la CP o quede fuera del comercio siempre y cuando Proveedor de Certificados PROCERT, C.A. no se encuentre en mora.

En lo adelante cada una de las referidas condiciones serán denominadas individualmente como causa extraña no imputable o fuerza mayor y activarán los planes de recuperación ante desastres y continuidad de negocio de Proveedor de Certificados PROCERT, C.A. Si se presenta una causa extraña no imputable o fuerza mayor Proveedor de Certificados PROCERT, C.A. notificará a los Signatarios explicando detalladamente el evento, así como el grado hasta el cual el mismo afectará el cumplimiento

de sus obligaciones bajo esta CPS o la CP. Durante el periodo de duración del evento que califique como causa extraña no imputable o fuerza mayor Proveedor de Certificados PROCERT, C.A. procurará encontrar medios alternos que le permitan cumplir las obligaciones asumidas bajo la CPS o la CP, y atemperar cualquier efecto o impacto negativo derivado de la causa extraña no imputable o fuerza mayor sobre la prestación del servicio de certificación electrónica. Al concluir el evento que califique como causa extraña no imputable o fuerza mayor, Proveedor de Certificados PROCERT, C.A. notificará a los Signatarios y se continuará con la prestación del servicio. Si el evento que califique como causa extraña no imputable o fuerza mayor no cesare dentro del plazo de treinta (30) días calendario, siguientes a la fecha de notificación a los Signatarios, Proveedor de Certificados PROCERT, C.A. procederá al cese de operación notificando a tales fines a la SUSCERTE, los Signatarios e iniciando el proceso de entrega a la SUSCERTE de la RPKI para su operación.

9.16.6. Otras estipulaciones.
No se contemplan.

10. Referencias normativas.
- Webtrust (Enlace web de cumplimiento)
- CA Browser Fórum (Enlace web de cumplimiento)
- Decreto ley de mensaje de datos y firmas electrónicas y su reglamento.
- Normativa de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).
- Normativa PROCERT.
- Estándar internacional ITU- T X.500.
- Estándar internacional ITU- T X.509 V3.
- Estándar Internacional ITU-T X.609.
- Norma ISO 9001:2015.
- Norma ISO/IEC 9594-8.
- Norma ISO/TR 10013:2021.
- Norma ISO/IEC 27001:2022.
- Norma ISO/IEC 27002:2022
- Norma ISO/IEC 27002:2022
- 27011:2022
- RFC 5280.
- RFC 6484.
- RFC 6485.
- RFC 6487.
- FIPS 140-2
- FIPS 140-3